EXHIBIT A

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYSTEMS, INC.,
Petitioner,

v.

MONEY AND DATA PROTECTION LIZENZ GMBH & CO. KG
Patent Owner

IPR2019-01638
U.S. Patent No. 9,246,903

PETITION FOR *INTER PARTES* REVIEW UNDER 35 U.S.C. §312 AND 37 C.F.R. §42.104

Claims 1-3, 5-8, and 10-13

TABLE OF CONTENTS

PETITIONER'S EXHIBIT LIST

September 24, 2019

Ex-1001	U.S. 9,246,903
Ex-1002	Prosecution History of U.S. 9,246,903
Ex-1003	Declaration of Patrick McDaniel, Ph.D., under 37 C.F.R. §1.68
Ex-1004	*Curriculum Vitae* of Patrick McDaniel, Ph.D.
Ex-1005	U.S. Patent No. 8,862,097 to Brand et al.
Ex-1006	U.K. Patent Application 2,398,159 to Williams
Ex-1007	U.S. Patent No. 9,647,855 to Deibert
Ex-1008	U.S. Publication No. 2011/0202466 to Carter
Ex-1009	U.S. Patent No. 6,182,229 to Nielsen
Ex-1010	WO 2009/089943 by Dietrich et al.
Ex-1011	*Reserved*
Ex-1012	*Reserved*
Ex-1013	*Reserved*
Ex-1014	U.S. Patent No. 7,039,392 to McCorkle et al.
Ex-1015	U.S. Patent No. 8,245,292 to Buer
Ex-1016	*Reserved*
Ex-1017	*Reserved*
Ex-1018	*Reserved*
Ex-1019	*Reserved*

Ex-1020	Patrick McDaniel. Computer and Network Authentication. *Handbook of Information Security*, John Wiley and Sons. September 2006. *Editor*: Hossein Bidgoli. URL: http://patrickmcdaniel.org/pubs/mcdaniel-netauth.pdf
Ex-1021	Patrick McDaniel. Authentication. *The Internet Encyclopedia*, John Wiley and Sons. 2002. URL: http://patrickmcdaniel.org/pubs/mcdaniel-authentication.pdf
Ex-1022	Anthony Nicholson, Mark D. Corner, and Brian D. Noble, "Mobile Device Security using Transient Authentication," *IEEE Transactions on Mobile Computing*, 5(11):1489–1502, November 2006.
Ex-1023	English translation of WO 2009/089943 to Dietrich et al.
Ex-1024	Information Disclosure Statement submitted in U.S. App. No. 12/334,957 on June 3, 2009.

I. INTRODUCTION

Pursuant to 35 U.S.C. §§ 311, 314(a), and 37 C.F.R. § 42.100, Cisco Systems, Inc. ("Petitioner") respectfully requests that the Board review and cancel as unpatentable under (pre-AIA) 35 U.S.C. §103(a) claims 1-3, 5-8, and 10-13 (hereinafter, the "Challenged Claims") of U.S. 9,246,903 ("'903 Patent," Ex-1001).

The '903 Patent describes two-factor authentication technology for authenticating a user to a transaction. As shown below and in the Declaration of Patrick McDaniel (Ex-1003), these concepts were well-known before the '903 Patent was filed. The primary reference ("Brand," Ex-1005) describes a two-factor authentication system. The other claimed concepts—such as deactivating an application, estimating location, transmitting data over different networks, and identity tokens—were also well-known. The combination of prior art concepts in the Challenged Claims was obvious.

II. MANDATORY NOTICES

A. Real Party-in-Interest

Pursuant to 37 C.F.R. § 42.8(b)(1), Petitioner certifies that the real parties-in-interest are Cisco Systems, Inc. and Duo Security, Inc.

B. Related Matters

Pursuant to 37 C.F.R. § 42.8(b)(2), to the best knowledge of the Petitioner,

the ’903 Patent is involved in the following cases:

Case Heading	Number	Court	Filed
Money and Data Protection Lizenz GmbH & Co. KG v. Duo Security, Inc.	1-18-cv-01477	DED	September 25, 2018

Petitioner is also concurrently filing a petition for *inter partes* review of claims 14-17, 19, 21-22, and 24-26 of the ’903 Patent.

C. Lead and Back-up Counsel and Service Information

Lead Counsel
David L. McCombs
HAYNES AND BOONE, LLP
2323 Victory Ave. Suite 700
Dallas, TX 75219
Phone: (214) 651-5533
Fax: (214) 200-0853
david.mccombs.ipr@haynesboone.com
USPTO Reg. No. 32,271

Back-up Counsel
Theodore M. Foster
HAYNES AND BOONE, LLP
2323 Victory Ave. Suite 700
Dallas, TX 75219
Phone: (972) 739-8649
Fax: (214) 200-0853
ipr.theo.foster@haynesboone.com
USPTO Reg. No. 57,456

Dina Blikshteyn
HAYNES AND BOONE, LLP
2323 Victory Ave. Suite 700
Dallas, TX 75219
Phone: (212) 835-4809
Fax: (214) 200-0853
dina.blikshteyn.ipr@haynesboone.com
USPTO Reg. No. 63,962

Please address all correspondence to lead and back-up counsel. Petitioner consents to service in this proceeding by email at the addresses above.

III. GROUNDS FOR STANDING

Petitioner certifies that the ’903 Patent is eligible for *inter partes* review

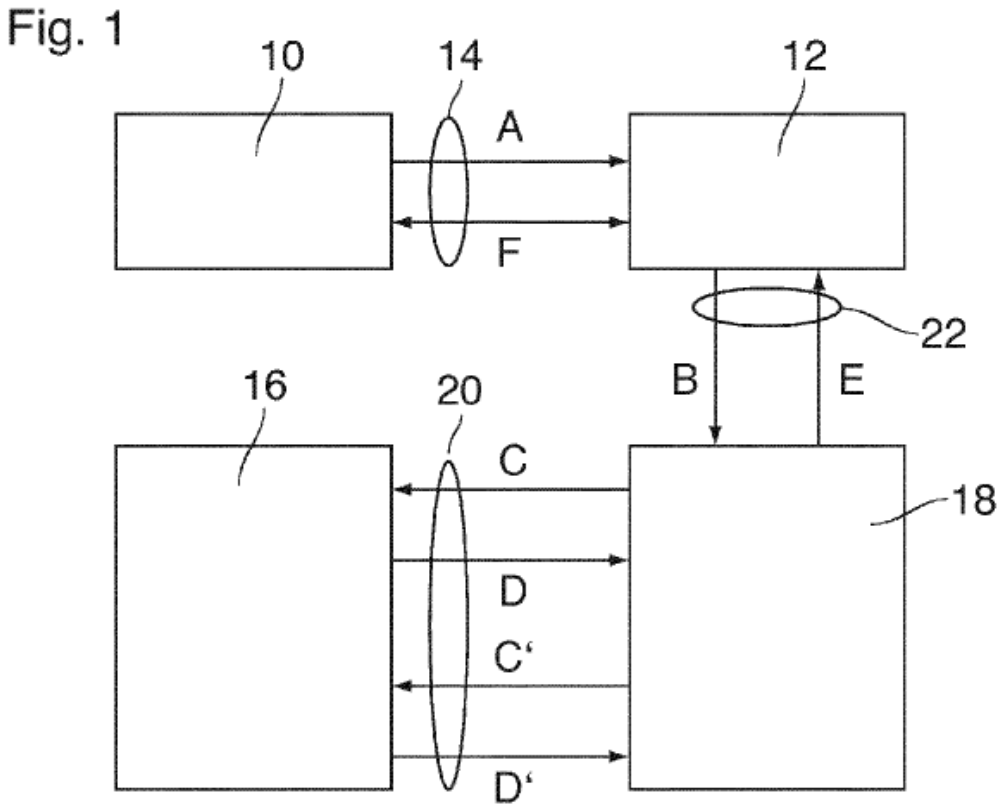
("IPR") and that Petitioner is not barred or estopped from challenging the patent claims on the grounds identified. 37 C.F.R. § 42.104(a).

IV. NOTE

Unless otherwise noted, all emphasis in any quoted material has been added.

V. '903 PATENT

The '903 Patent describes "authenticating a user to a transaction." Ex-1001, 1:3-4. The authentication system, illustrated in Fig. 1 below, includes transaction terminal 10, remote transaction partner 12, mobile communication device 16, and authentication device 18. Ex-1001, 4:41-45. Up to three separate communication channels (14, 20, 22) link the components. Ex-1001, 4:39-49.



Ex-1001, FIG. 1

A user "operates the terminal 10 and sends a transaction request to the transaction partner 12." Ex-1001, 4:57-60; FIG. 1 (A). The request includes a "user-ID." Ex-1001, 4:60-61. "[T]he transaction partner 12 forwards the user-ID to the authentication device 18." Ex-1001, 4:61-63, FIG. 1 (B). The "authentication device 18 retrieves the mobile telephone number and or the IMSI of the user and contacts the mobile device 16" to check whether an "authentication function... is active." Ex-1001, 4:63-5:1, FIG. 1 (C). When the authentication device 18 confirms "that the authentication function is active, the authentication device 18 sends an authentication signal to the transaction partner 12." Ex-1001, 5:1-3, FIG.

1 (D & E). The authentication signal "informs the transaction partner that this specific user is authenticated to the requested transaction." Ex-1001, 5:4-7. The transaction is then "performed via the terminal 10." Ex-1001, 5:7-9, FIG. 1 (F).

VI. LEVEL OF ORDINARY SKILL

A Person of Ordinary Skill in The Art ("POSITA") in October 2011 would have had a working knowledge of the authentication art that is pertinent to the '903 Patent, including two-factor authentication using a mobile device. A POSITA would have had a bachelor's degree in computer science, computer engineering, or an equivalent, and three years of professional experience. Lack of professional experience can be remedied by additional education, and vice versa. Ex-1003, ¶¶ 15-19.

VII. CLAIM CONSTRUCTION

This Petition analyzes claims according to their ordinary and customary meaning as would be understood by one of ordinary skill in the art in view of the specification. *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (*en banc*); Ex-1003, ¶¶ 49-50.

Various claims recite features using language that approximates Markush-style claiming of alternatives. *See* M.P.E.P. 2117. For the reasons below, in this proceeding these quasi-Markush terms are construed as reciting a list of alternatives.

A. "deactivating the authentication function after a predetermined time interval after at least one of: activation thereof and when an active state thereof has been checked."

This limitation is recited in claim 2. The '903 Patent describes two alternative embodiments, shown in Figs. 3 and 4, in which an authentication application is deactivated based on timers that are started by different events. Ex-1001, 5:46-6:13. Accordingly, the plain and ordinary meaning, in light of the specification, of this limitation is: *deactivating the authentication function after a predetermined time interval after (1) activation thereof,* or *(2) when an active state thereof has been checked.* Ex-1003, ¶ 51.

B. "the steps of one of storing and generating the password in the mobile device and transmitting the password to the authentication device."

This limitation is recited in claim 11. The '903 Patent describes how a "password may be stored permanently in the mobile device" and then "sent to the authentication device." Ex-1001, 10:5-7. The '903 Patent further provides that "instead a password generator" generates a password which is then "sent via the communication channel." Ex-1001, 10:8-17. Accordingly, the plain and ordinary meaning, in light of the specification, of this limitation is: *(1) storing the password in the mobile device and transmitting the password to the authentication device,* or *(2) generating the password in the mobile device and transmitting the password to the authentication device*. Ex-1003, ¶ 52.

C. "the step of one of storing and converting the password in the authentication device."

This limitation is recited in claim 12. The '903 Patent describes "a universal password that is used for each authentication process regardless of the transaction partner and the type of service involved." Ex-1001, 10:17-21. If "the authentication is successful, the authentication device 18 automatically converts the universal password into a specific password that is pertinent for the type of service." Ex-1001, 10:23-27. Accordingly, a plain and ordinary meaning of this limitation in light of the specification is: *(1) storing the password in the authentication device* or *(2) converting the password in the authentication device*. Ex-1003, ¶¶ 53-55.

VIII. RELIEF REQUESTED AND REASONS THEREFORE

Petitioner asks that the Board institute a trial for *inter partes* review of the Challenged Claims and cancel these claims.

IX. IDENTIFICATION OF HOW THE CLAIMS ARE UNPATENTABLE

A. Challenged Claims

This Petition challenges claims 1-3, 5-8, and 10-13 of the '903 Patent.

B. Statutory Grounds for Challenges

Ground	Claim(s)	Basis
#1	1, 2, and 3	35 U.S.C. § 103 (Pre-AIA) over Brand, Williams, and Deibert
#2	5, 6, 7, 8, 10, and 11	35 U.S.C. § 103 (Pre-AIA) over Brand, Williams, Deibert, and Carter
#3	11, 12	35 U.S.C. § 103 (Pre-AIA) over Brand, Williams, Deibert, Carter, and Nielsen
#4	13	35 U.S.C. § 103 (Pre-AIA) over Brand, Williams, Deibert, and Dietrich

U.S. Patent No. 8,862,097 to Brand (Ex-1005, "Brand") was filed on December 3, 2009.

U.K. Patent Application GB2,398,159 to Williams (Ex-1006, "Williams") published on August 11, 2004. Williams' publication status is confirmed by its citation on an Information Disclosure Statement by the applicants in U.S. App. No. 12/334,957 on June 3, 2009. *See* Ex-1024.

U.S. Patent No. 9,647,855 to Deibert (Ex-1007, "Deibert"), was filed on January 9, 2008.

U.S. Publication No. 2011/0202466 to Carter (Ex-1008, "Carter"), was filed on October 19, 2009.

U.S. Patent No. 6,182,229 to Nielsen (Ex-1009, "Nielsen"), was published on January 30, 2001.

WO 2009/089943 by Dietrich (Ex-1010, "Dietrich") was published on July 23, 2009. Petitioner cites to the English translation of Dietrich (Ex-1023) submitted to the Office in U.S. Application No. 12/811,549 on July 2, 2010.

Brand, Deibert, and Carter are prior art under 35 U.S.C. § 102(e).

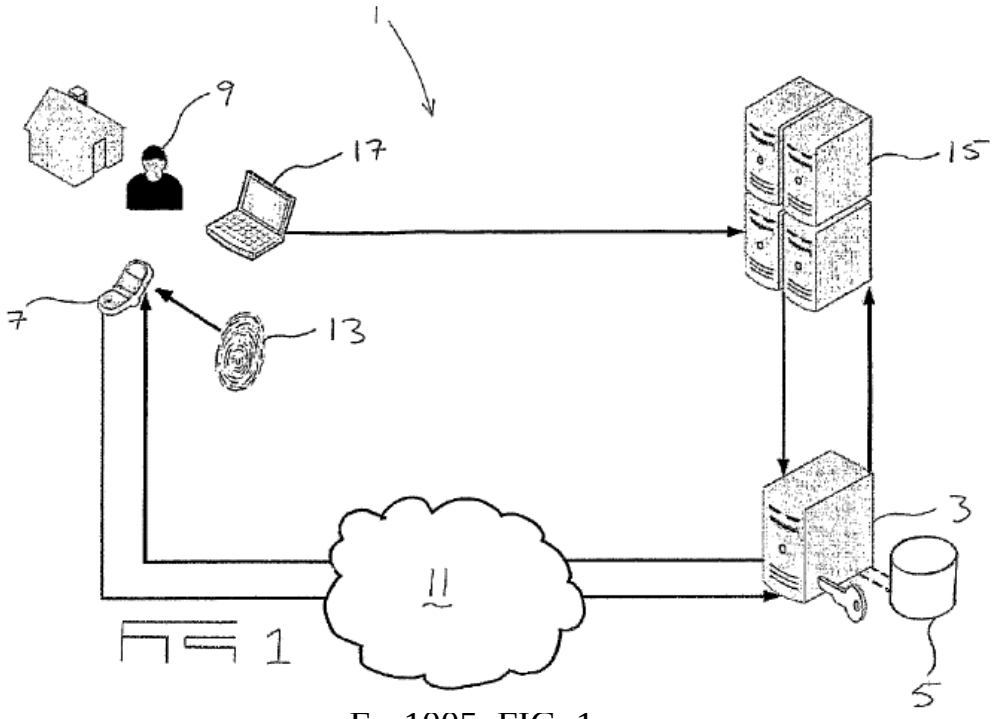
Williams, Nielsen, and Dietrich are prior art under 35 U.S.C. § 102(b).

Petitioner's proposed combinations permit but do not require the physical incorporation of elements. *See In re Mouttet*, 686 F.3d 1322, 1332 (Fed. Cir. 2012); Ex-1003, ¶ 64.

C. Ground 1: Claims 1, 2, and 3 are obvious over Brand, Williams, and Deibert

1. Brand

Like the '903 Patent, Brand (Ex-1005) discloses a system "for authenticating secure transactions between a transacting user and a secure transaction host." Ex-1005, Abstract. Figure 1 (below) shows Brand's authentication system including a user (9), user's computer (17), banking institution (15), user's mobile phone (7), and authentication server (3). Ex-1005, 5:44, 6:48-55.



Ex-1005, FIG. 1

Brand discloses that "to log into his or her internet banking account, the user (9) first accesses the website of the banking institution (15) at which his or her account is held, from a personal computer (17), laptop or other Internet enabled device." Ex-1005, 6:47-50. The user "enters his account number (equivalent to a username) and password on the Internet banking website on his computer." Ex-1005, 6:50-53.

"Before proceeding to login, the user (9) initiates the authentication application on his/her mobile phone." Ex-1005, 6:53-55. The authentication application establishes a "real-time communication link" via "a GSM network"

between "the authentication server" and "the mobile phone." Ex-1005, 6:62-64, 5:67.

"Upon the user (9) requesting login to his internet banking account, the banking institution (15) requests authentication of the user (9) from the authentication server." Ex-1005, 7:1-3. The authentication server "sends a transaction confirmation request to the mobile phone (7) which is received by the software application." Ex-1005, 7:3-6. The "software application triggers a pop-up on the monitor of the mobile phone" which allows "the user (9) to either confirm (accept) or deny (reject) the transaction." Ex-1005, 7:6-12.

If the user "confirms the transaction, the application communicates this confirmation result to the server" which "sends a positive authentication result to the banking institution server." Ex-1005, 7:12-15. The banking institution then allows the user "to proceed to its Internet banking account." Ex-1006, 7:15-17.

2. Williams

Like Brand, Williams relates to "a transaction authorisation[1] system for electronic payments." Ex-1006, 8. Williams teaches that terminals are "linked to a card issuer's central transaction processing unit." Ex-1006, 8. The transaction processing unit has an authorisation module which causes a message generation

[1] As a U.K. patent, Williams uses British English spellings.

module to transmit "a SMS message identifying the card account, the transaction data and time, the merchant and the transaction value..." to "a mobile communication device... for the card account." Ex-1006, 9. The account holder "sends a return SMS message... using his mobile device." Ex-1006, 10. If the "return SMS message is received within a predetermined period of time, the authorisation module 3 instructs the transaction processing unit to authorise the transaction." Ex-1006, 11.

3. Deibert

Deibert relates to mobile device payments. Ex-1007, Abstract. Deibert describes "mobile payment applications." Ex-1007, 6:45-48. An application includes "a timer that automatically deactivates any mobile payment application[] after a predetermined timeout time has elapsed." Ex-1007, 6:50-52.

4. Reasons to Combine Brand and Williams

A POSITA would have found it obvious to combine the teachings of Brand and Williams for multiple reasons, including to obtain predictable and beneficial results that validate that the user possesses the mobile device while conducting a transaction. Ex-1003, ¶ 75.

First, a POSITA, when considering the teachings of Brand, would have also considered the teachings of Williams since they are analogous prior art pertaining

specifically to payment transaction authorization and two-factor authentication. Ex-1005, Abstract, 10:59-62; Ex-1006, Abstract, 8-11; Ex-1003, ¶ 76.

Second, the two authentication factors in Brand are "something the person to be authenticated has" (*e.g.*, a mobile device) and "something he or she knows (for example a username and password)." Ex-1005, 2:40-44. Requiring "the user to interactively confirm (accept) or deny (reject) the transaction" validates that the user possesses the mobile device. Ex-1005, 10:46-48. A POSITA would have recognized such techniques are desirable, as they increase the authentication system's security and reduce fraud where a third-party, acting as a user, initiates a transaction. Ex-1003, ¶ 77.

Williams similarly describes authenticating a transaction via a user's mobile phone. Ex-1006, Abstract. When a transaction is requested, Williams' system sends an SMS message to the user's mobile phone. Ex-1006, 10. The transaction is authorized only if the user's "return SMS message" is "received within a predetermined period of time." Ex-1006, 11.

A POSITA would have recognized that Williams' predetermined period of time during which a transaction may be authorized improves the security of Williams' system and assists in preventing the authorization of fraudulent transactions. Ex-1003, ¶ 79. Without any such time limit, a requested transaction would remain pending until the user responds. This could lead to the user

unintentionally or mistakenly approving a transaction that the user did not request (i.e., a fraudulent transaction). Ex-1003, ¶ 79.

It would have been obvious to a POSITA to employ a similar time limit in Brand's system, such that a user would have a limited period of time to validate that the user possesses the mobile device. Ex-1003, ¶ 79. This would contribute to the overall security of the authentication system. Including a predetermined time period is a way to validate that the user possessed the mobile device between the time the user initiated the transaction at his computer and the transaction was confirmed (or denied) at the authentication server. Ex-1003, ¶ 80; Ex-1005, 10:48-50. If the authentication server has not received a confirmation message after the predetermined time interval expired, the authentication server would determine that the transaction is fraudulent. Ex-1003, ¶ 80. When a user does not approve a transaction in a timely manner, there is an increased risk that the transaction is fraudulent. Ex-1003, ¶ 80. More generally, it was known in the art that security is enhanced "by limiting the time when authentication is possible." Ex-1014, 17:4-5.

Third, such a combination would have simply been combining prior art elements (Williams' time-limited window for responding and Brand's accept/deny message) according to known methods (rejecting transactions for which a timely response is not received) to yield predictable results (validating that the user possesses the mobile device at the time of a transaction). Ex-1003, ¶ 81.

Additionally, the combination of Brand and Williams is merely the ordinary use of a common technique (limiting the time window for approving a transaction) to improve a similar two-factor authentication system in the same way (reducing fraudulent transactions). Ex-1003, ¶ 81.

5. Reasons to Combine Brand and Deibert

A POSITA would have found it obvious to combine the teachings of Brand and Deibert for multiple reasons, including to produce the obvious, beneficial, and predictable result of automatically deactivating the authentication application. Ex-1003, ¶ 83.

First, a POSITA, when considering the teachings of Brand, would have also considered the teachings of Deibert since they are analogous prior art pertaining to payment systems. Ex-1005, Abstract; Ex-1007, Abstract. Both Brand and Deibert describe authentication features that prevent fraud. Ex-1005, Abstract; Ex-1007, 9:27-30; Ex-1003, ¶ 84.

Second, Brand teaches that a user "initiates the authentication application on his/her mobile phone." Ex-1005, 6:53-54. A POSITA would have recognized that once initiated, the authentication application would execute on mobile device until the application is deactivated or the mobile device loses power. Ex-1003, ¶ 85. During that time, the authentication application would consume resources including battery power. Accordingly, a POSITA would have recognized that

automatically deactivating the authentication application would have been desirable. Ex-1003, ¶ 85.

Deibert teaches software "code relating to a timer that automatically deactivates any mobile payment applications." Ex-1007, 6:49-53. A POSITA would have been motivated to combine Deibert's teachings that describe the deactivation code with Brand's authentication application so that the authentication application would deactivate automatically. Ex-1003, ¶ 86. In this way, the authentication application does not needlessly execute on the mobile device and consume system resources, *e.g.*, the processor, memory, and battery (which can be used to process other applications). Ex-1003, ¶ 87. Automatically deactivating the authentication application would also make the application easier to use because the user would not have to remember to manually deactivate the application after accepting (or denying) the transaction. Ex-1003, ¶ 88. Additionally, if a user has a predetermined period of time during which a user can authenticate a transaction, it would have been obvious to a POSITA for the authentication application to automatically deactivate after the amount of the predetermined period of time expired, since any response would be untimely and therefore moot. Ex-1003, ¶ 88.

Third, Deibert describes "code relating to a timer that automatically deactivates... applications after a predetermined timeout time has elapsed." Ex-1007, 6:49-53. A POSITA would have been motivated to include a timer that

begins to count down for a predetermined time before deactivating Brand's authentication application. Ex-1003, ¶ 89. This would beneficially save resources of the mobile device. Ex-1003, ¶ 89. This would also increase security of the authentication system, because once deactivated, the authentication application would require the user to reinitiate the application using user's credentials and prevent a third-party from using the authentication application. Ex-1005, 6:53-55, 8:51-56; Ex-1003, ¶ 89. Confirming this, Brand teaches that "a person who comes into possession of the mobile phone illegally will not even be able to activate the software application, let alone establish the communications link with the authentication server." Ex-1005, 8:53-56.

A POSITA looking to implement the deactivation code would recognize that the predetermined time period would need to start upon the occurrence of some event. Ex-1003, ¶ 90. An obvious event to start a timer would be when the authentication application is initiated. Ex-1003, ¶ 90; Ex-1005, 6:53-55. In this case, the timer would be long enough for the user to authenticate a transaction. Another obvious event would be when the authentication server received a message confirming/denying the transaction, since at that point the authentication application has fulfilled its purpose. Ex-1003, ¶ 90; Ex-1005, 6:53-55; 7:12-13, 7:25-29. Either of those events would allow the user to authenticate the transaction

while safeguarding the security of the authentication system and preserving resources of the mobile device. Ex-1003, ¶ 90.

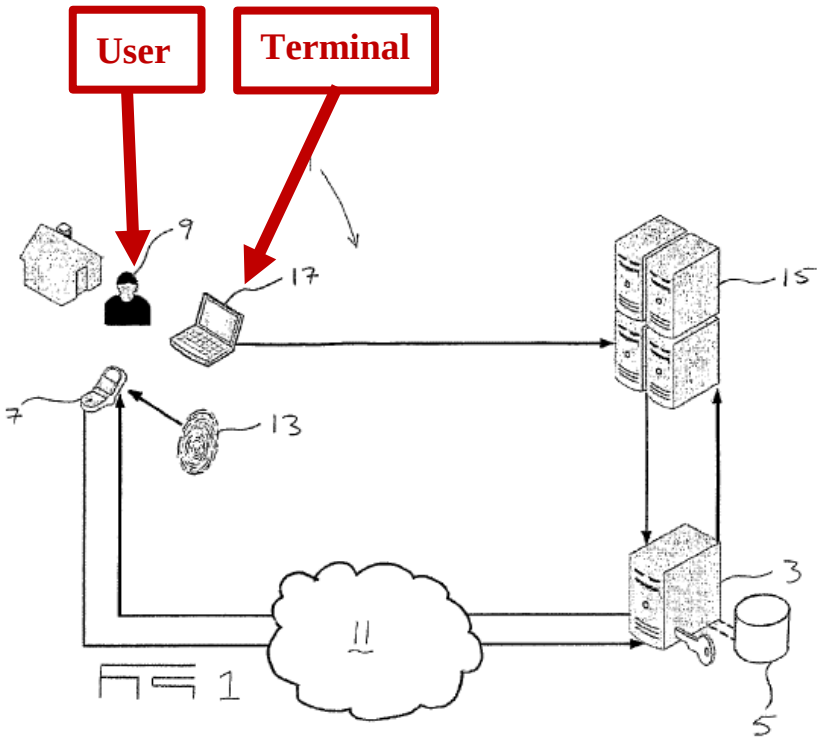
Fourth, a POSITA would have been familiar with conventional coding languages, such as Java, C++ or Perl, used to write software applications. Ex-1003, ¶ 91; *see also* Ex-1007, 10:47-50; Ex-1005, 9:25-26, 9:40-46; Ex-1001, 4:52-53, 6:22-38. A POSITA would have considered this information when using Deibert's code that "automatically deactivates" an application after a predetermined time period has lapsed with Brand's authentication application. Ex-1003, ¶ 91. The combination is simply combining prior art elements (Deibert's timer that automatically deactivates Brand's authentication application) according to known methods (code written in a programming language) to yield predictable results (automatically deactivating the authentication application). Ex-1003, ¶ 91.

6. Claim 1

[1.0] ***A method of authenticating a user to a transaction at a terminal, comprising the steps of:***

Brand discloses the preamble. Brand discloses "[a] ***method***... **for *authenticating* secure *transactions* between a transacting *user*** and a secure transaction host." Ex-1005, Abstract. Brand further discloses that the user performs a log-in process (a *transaction*) from a *terminal* such as "**a personal computer**

(17), laptop or other Internet enabled device." Ex-1005, 6:47-50; Ex-1003, p. 43. Brand's system is shown in Figure 1:



Ex-1005, FIG. 1 (Annotated); Ex-1003, p. 44.

Accordingly, Brand discloses a method of authenticating a user to a transaction conducted on a computer, which discloses "*[a] method of authenticating a user to a transaction at a terminal.*" Ex-1003, p. 44.

[1.1] ***transmitting a user identification from the terminal to a transaction partner via a first communication channel;***

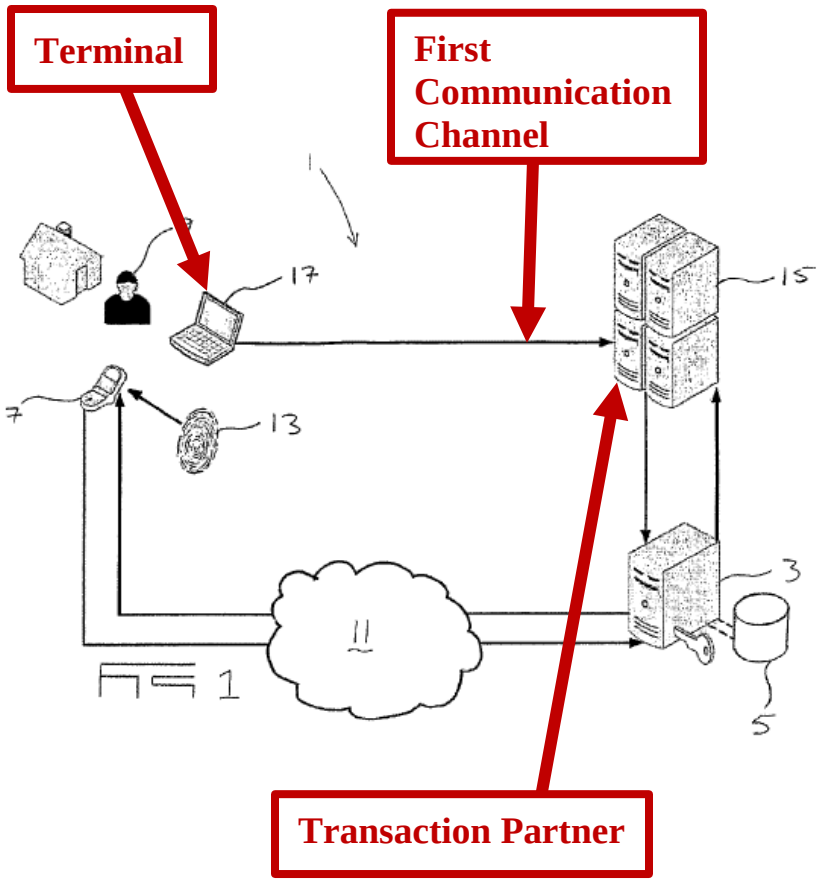
Brand discloses this limitation. First, Brand discloses the user "requesting login to his internet banking account" at a banking institution. Ex-1005, 7:1-3. The user logs in by "enter[ing] his **account number (equivalent to a username) and**

password on the Internet banking website **on his computer**." Ex-1005, 6:51-53. The user's account number is a *user identification* because it identifies the user to a banking institution, and the banking institution operating the Internet banking website is a *transaction partner*. Ex-1003, pp. 44-45; Ex-1006, 1:47-53. As discussed in [1.0], the user's computer is the *terminal*. Ex-1003, p. 46.

Brand discloses that the account number is *transmit[ted]* to the banking institution because "the banking institution (15) requests authentication of the user" upon user logging in by entering "his account number... and password." Ex-1005, 7:1-3, *see also id.* 66:50-53, Fig. 1 (line from 17 to 15); Ex-1003, p. 45. It would have been obvious that the account number and password are transmitted to the banking institution. Ex-1003, p. 45.

Second, Brand discloses that the user "first accesses **the website of the banking institution**... from a personal computer (17), laptop or other **Internet enabled device**." Ex-1005, 6:48-50. The Internet connection between the user's computer and the banking institution is *a first communication channel*. Ex-1003, ¶ p. 45.

Brand's Figure 1 illustrates the computer (*terminal*), the banking institution (*transaction partner*), and an Internet enabled connection between the computer and the banking institution (*first communication channel*). Ex-1005, Figure 1.



Ex-1005, FIG. 1 (Annotated); Ex-1003, p. 46.

Accordingly, Brand discloses transmitting an account number (username) over an Internet connection from the user's computer to the banking institution, which discloses "*transmitting a user identification from the terminal to a transaction partner via a first communication channel*." Ex-1003, p. 46.

[1.2] ***providing an authentication step in which an authentication device uses a second communication channel for checking an authentication function that is implemented in a mobile device of the user,***

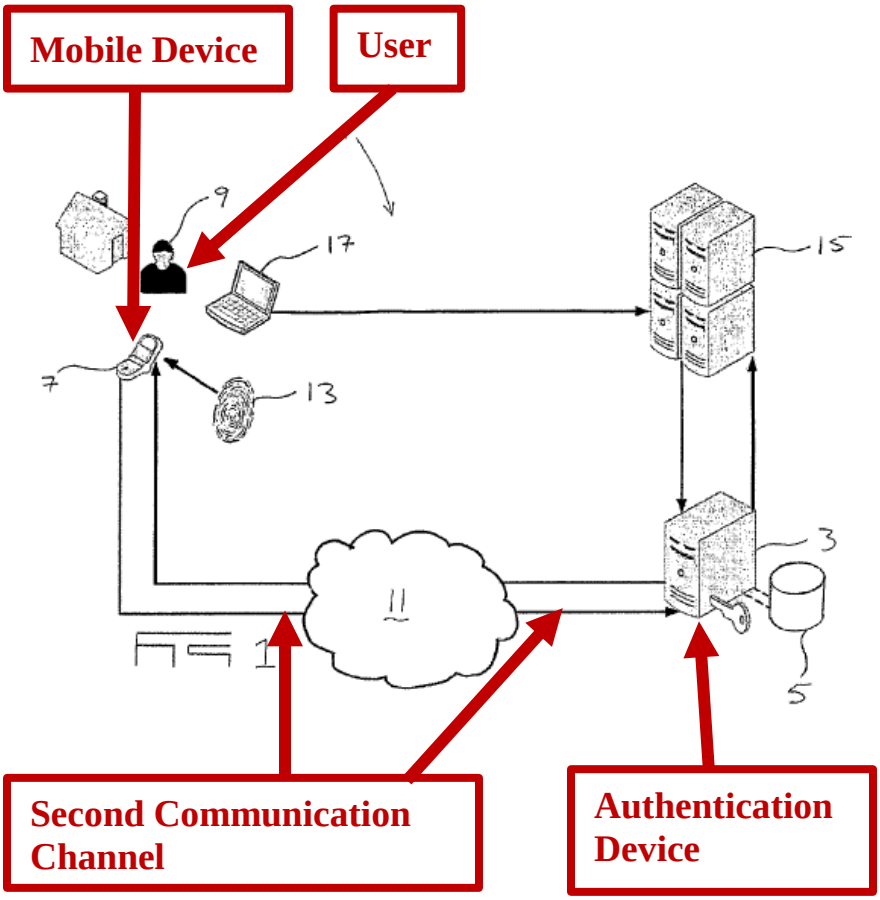
Brand discloses this limitation. First, Brand discloses *an authentication step* where "the banking institution (15) requests authentication of the user (9) from the

authentication server." Ex-1005, 7:1-3. The authentication server is *an authentication device*. Ex-1003, pp. 46-47.

During the *authentication step*, "the **authentication server (3)** in turn **sends a transaction confirmation request to the mobile phone (7) which is received by the software application**." Brand, 7:3-6. Brand discloses that "the user (9) initiates the **authentication application**" (*authentication function*) "**on his/her mobile phone**," which is "*a mobile* communication *device*." Ex-1005, 6:53-54; 5:46-48; Ex-1003, p. 47. Thus, the authentication application on the mobile phone discloses *an authentication function that is implemented in a mobile device of the user*. Ex-1003, pp. 47-48.

Second, Brand discloses that a "**[c]ommunication between the application on the mobile phone (7) and the authentication server (3) takes place via a GSM network**" which provides a "real-time communication link." Ex-1005, 5:65-6:3, 6:53-54. The GSM network communication link is *a second communication channel*. Ex-1003, p. 48.

Brand's Figure 1 (below) illustrates an authentication server (*authentication device*), a mobile phone (*mobile device*) of a *user*, and a GSM network communication link (*second communication channel*):



Ex-1005, FIG. 1 (Annotated); Ex-1003, p. 49.

Accordingly, Brand discloses an authentication server that authenticates a user by sending a request over a GSM network communication link to an authentication application in a user's mobile device, which discloses "*providing an authentication step in which an authentication device uses a second communication channel for checking an authentication function that is implemented in a mobile device of the user*." Ex-1003, p. 49.

[1.3.1] ***as a criterion for deciding whether the authentication to the transaction shall be granted or denied, having the authentication device check whether a predetermined time relation exists ...***

Brand and Williams render this limitation obvious. First, Brand discloses authentication where a pop-up of the authentication application "requests the user (9) to either confirm (accept) or deny (reject) the transaction by means of an appropriate key press," and communicates a "result to [authentication] server." Ex-1005, 7:6-13, 7:25-27. The authentication server (*authentication device*) checks the result because the server sends a corresponding positive or negative "authentication result" to a banking institution. Ex-1005, 7:13-15, 7:25-29; 8:25-32. Ex-1003, pp. 49-50.

Second, Williams, which like Brand authenticates the user, teaches an authorisation module that causes an SMS message "identifying the card account, the transaction data and time, the merchant and the transaction value" to be sent "to the account holder's nominated mobile device." Ex-1006, 9-10. The authorisation module *check[s]* if a "**return SMS message is received within a predetermined period of time**," which is a *criterion*. Ex-1006, 11. If so, *the transaction shall be granted* because "the authorisation module 3 instructs the transaction processing unit 2 to **authorise the transaction**." Ex-1006, 11. "[I]f no such SMS message is received within this time, **the transaction is not authorised**," and *the transaction shall be denied*. Ex-1006, 11. The predetermined period of time taught in Williams

is *a predetermined time relation* which is checked "*for deciding whether the authentication to the transaction shall be granted or denied*." Ex-1003, p. 51.

It would have been obvious to a POSITA for Brand's authentication server to check if a user's response is received within a predetermined time period, as taught by Williams. Ex-1003, p. 52. First, it would make the transaction more secure by validating that the user possessed the mobile device when he initiated the transaction at the terminal. Ex-1003, p. 52. Second, it would reduce fraudulent transactions because the authentication server would not authenticate transactions after the predetermined time period expired. Ex-1003, p. 52. *See* Reasons to Combine Brand and Williams, § IX.C.4.

Accordingly, Brand and Williams teach an authentication server that checks whether an authorization response was received during a predetermined time period, which renders obvious "*as a criterion for deciding whether the authentication to the transaction shall be granted or denied, having the authentication device check whether a predetermined time relation exists*." Ex-1003, p. 52.

[1.3.2] [a predetermined time relation exists] between the transmission of the user identification and a response from the second communication channel,

Brand and Williams render this limitation obvious. First, as discussed in [1.1], Brand discloses that the *terminal* transmits *user identification*. Ex-1003, p. 52.

Second, Brand discloses an authentication application communicating a confirmation or denial "result" (*response*) to the authentication server (*authentication device*). Ex-1005, 7:12-13, 7:25-29; Ex-1003, pp. 52-53.

Third, Williams teaches a user "entering data concerning a transaction," e.g. a card name and number, and then transmitting a "notification message to a predetermined mobile communication device." Ex-1006, 6. The user "reads the SMS message on his screen 7, and if it corresponds to a transaction of which he is aware, he sends a return SMS message." Ex-1006, 10. The authorisation module checks if "an appropriate return SMS message is received within a predetermined period of time." Ex-1006, 11. It would have been obvious to a POSITA that this "predetermined period of time" would be measured from when the transaction was first initiated, i.e., starting at *the transmission of the user identification*. Ex-1003, p. 54. For example, if the *relation* between the time that the user enters data (e.g. card name and number) and the time the user sends a return SMS message that confirms the transaction is within the predetermined time period (*predetermined time*), the

transaction is authorised. Ex-1003, p. 54. Alternatively, if a *relation* between the time the user enters data and the time the user sends a return SMS message is greater than the predetermined time period, the transaction is denied. Ex-1003, p. 54; Ex-1006, 11.

Fourth, as discussed in [1.2], Brand discloses that the mobile device and the authentication server communicate via a GSM network communication link (*second communication channel*). Thus, *the response* transmitted from the mobile device's authentication application to the authentication server is transmitted over the *second communication channel*. Ex-1003, pp. 54-55.

It would have been obvious to a POSITA to determine whether the time that Brand's user transmitted user information to the banking institution and the time the user transmitted a confirmation or denial result to the authentication server falls within the predetermined time period taught in Williams. Ex-1003, p. 55. This would make the authentication system more secure by adding a safeguard that validates that a person possessed the mobile device when the transaction was initiated and authenticated. It would also reduce fraudulent transactions because transactions would not authenticate if the time interval exceeds the predetermined time period. Ex-1003, p. 55. *See* Reasons to Combine Brand and Williams, § IX.C.4.

Accordingly, Brand and Williams teach permitting a transaction to be approved only during a limited time following the transaction's initiation, which renders obvious "*a predetermined time relation exists between the transmission of the user identification and a response from the second communication channel*." Ex-1003, p. 55.

[1.4] ***ensuring that the authentication function is normally inactive and is activated by the user only preliminarily for the transaction,***

Brand and Deibert render this limitation obvious. First, as discussed in [1.1], Brand discloses a *transaction* that a *user* initiated at a *terminal*, and as discussed in [1.2], Brand discloses an authentication application (*authentication function*). Ex-1003, p. 55.

Second, Brand discloses "[b]efore proceeding to login, the user (9) **initiates the authentication application** on his/her mobile phone." Ex-1005, 6:53-55. A POSITA would have understood that an authentication application was previously *inactive* because the user must initiate (*activate*) it. Ex-1003, pp. 55-56.

Third, in Brand the user initiates the authentication application "before proceeding to login" to the banking institution where the user conducts the transaction. Ex-1005, 6:53-54. Thus, Brand discloses "*ensuring that the authentication function... is activated by the user only preliminarily for the transaction*." Ex-1003, p. 56.

Fourth, Deibert teaches "a timer that **automatically deactivates** any mobile payment applications after a predetermined timeout time has elapsed." Ex-1007, 6:49-53. The "timer... begins counting down" when "the mobile phone is ready to conduct a transaction." Ex-1007, 9:35-38. A POSITA would have recognized that setting a timer that begins a countdown from a predetermined time period after an application is ready to conduct a transaction *ensure[s]* that the application is deactivated and "*is normally inactive*." Ex-1003, pp. 56-57

In light of Deibert's teachings, it would have been obvious to a POSITA for Brand's authentication application to include a timer that automatically deactivates the authentication application. Ex-1003, p. 57. This would make the authentication system more secure because a third-party who steals the user's mobile device would not be able to fraudulently authenticate a transaction without first initiating the authentication application. Ex-1003, p. 57. This also conserves mobile device resources. Ex-1003, p. 57. *See* Reasons to Combine Brand and Deibert, § IX.C.5.

Accordingly, Brand in combination with Deibert teaches that the authentication application is activated prior to proceeding with a login to conduct a transaction and is deactivated after a predetermined time period, which renders obvious "*ensuring that the authentication function is normally inactive and is activated by the user only preliminarily for the transaction*." Ex-1003, p. 57.

[1.5] ***ensuring that said response from the second communication channel includes information that the authentication function is active,***

Brand discloses this limitation. First, as discussed in [1.3.1], Brand discloses a result (*response*) transmitted from the authentication application (*authentication function*) to the authentication server via the GSM network communication link (*second communication channel*). Ex-1005, 7:12-15, 7:25-29; Ex-1003, p. 57. The authentication "application triggers a pop-up" through which the user confirms or denies the transaction, and then generates a "confirmation" or "denial" result. Ex-1005, 7:6-15, 7:25-29. Brand further explains that the pop-up to obtain a user's approval is optional. Ex-1005, 10:45-48 ("…a secure transaction ***may*** require the user to interactively confirm…"). It would have been obvious to a POSITA for the authentication application to be configurable to either present or suppress the individual transaction confirmation requests because Brand discloses that the pop-up behavior can be "configured." Ex-1005, 14:30-37; Ex-1003, pp. 58-59. Where the user has configured the authentication application to suppress the confirmation requests, the authentication application would immediately respond to the message received from the authentication server. Thus, the authentication application "provides a way of using a person's mobile phone to uniquely identify the user for authentication purposes" simply because the authentication application was active. *Cf*. Ex-1005, 10:48-50. Any of these potential response messages from the

authentication application to the authentication server would have demonstrated to the authentication server that the authentication application is *active*. Thus it would have been obvious to a POSITA for Brand's response message to *include[] information that the authentication function is active*. Ex-1003, pp. 58-59.

Second, Brand discloses that the authentication server checks that the authentication application is *active* because the authentication server receives and reads the result message from the authentication application to determine "if the authentication was successful." Ex-1005, 7:8-15, 7:25-29, 8:25-32; Ex-1003, p. 59. Based on the type of the result, the authentication server sends a "positive" or "negative" authentication result to the banking institution server. Ex-1005, 7:8-15, 7:27-29.

Accordingly, Brand discloses that the authentication application is used to generate a result and transmits the result to the authentication server which checks the result, which discloses "*ensuring that said response from the second communication channel includes information that the authentication function is active*," as claimed. Ex-1003, p. 59.

[1.6] ***thereafter ensuring that the authentication function is automatically deactivated.***

Brand and Deibert render this limitation obvious. First, as discussed in [1.2], Brand discloses an authentication application (*authentication function*) that

executes on a mobile device, and as discussed in [1.5], the authentication application generates a result (*information that the authentication function is active*). Ex-1003, p. 59.

Second, as discussed in [1.4], Deibert teaches a timer that "automatically deactivates" an application after a predetermined time. Ex-1006, 6:49-52. A POSITA would have recognized that such a timer would *ensure* that the application is *automatically deactivated*. Ex-1003, pp. 59-60.

In light of Deibert's teachings, it would have been obvious to a POSITA for Brand's authentication application to use a timer that automatically deactivates the authentication application after the authentication server receives a result that confirms or denies the transaction. Ex-1003, p. 60. This is because once the authentication server receives the result, the authentication application has fulfilled its purpose which is authenticating the user to a transaction. Ex-1003, p. 60. While the authentication application could deactivate immediately, a POSITA would have recognized that a user might perceive the sudden deactivation of the application as an abnormal termination (i.e., a "crash") of the application. Thus, a POSITA would have found it obvious for the authentication application to remain active for a short period of time so that it can provide a completion message to the user (e.g., "Authentication response successfully sent. This application will now close."). Ex-1003, p. 60. A POSITA would have recognized that Deibert's

deactivation timer would allow for this form of user interface feature, which improves the user's interaction with the authentication application. Ex-1003, p. 60. Deactivating the authentication application automatically would make the authentication application easier to use because the application is deactivated without user intervention, freeing up resources of the mobile device. Ex-1003, p. 60. *See* Reasons to Combine Brand and Deibert, § IX.C.5.

Accordingly, Brand and Deibert teach a timer that sets a predetermined timeout time to deactivate an authentication application after the authentication server receives a result, which renders obvious "*thereafter ensuring that the authentication function is automatically deactivated*." Ex-1003, p. 60.

7. Claim 2

[2.0] ***The method according to claim 1, wherein the step of thereafter ensuring that the authentication function is automatically deactivated***

See analysis at [1.0]-[1.6]. Ex-1003, p. 61.

[2.1] ***includes the step of deactivating the authentication function after a predetermined time interval after at least one of:***

Brand and Deibert render this limitation obvious. As discussed in [1.4], Deibert teaches "code relating to a timer that automatically **deactivates** any mobile payment applications **after a predetermined timeout time has elapsed**." Ex-1007, 6:49-52. The predetermined time out is a *predetermined time interval*. Ex-1003, p. 61.

It would have been obvious to a POSITA to use Deibert's deactivation timer to deactivate Brand's authentication application after a predetermined timeout time. Ex-1003, p. 61. This would make the authentication application easier to use because it would automatically deactivate without requiring user input after the predetermined time period expired. It would also free resources on the mobile device. Finally, it would make the authentication system more secure by requiring a user to reinitiate the authentication application to authenticate subsequent transactions. Ex-1003, pp. 61-62. *See* Reasons to Combine Brand and Deibert, § IX.C.5.

Accordingly, Brand and Deibert teach deactivating an authentication application after a predetermined timeout time, which renders this limitation obvious. Ex-1003, p. 62.

[2.2] ***[deactivating the authentication function after at least one of:] activation thereof and...***

As discussed in the claim construction section, the limitations in [2.2] and [2.3] are recited in the alternative, so a showing of either one in the prior art is sufficient to render the claim obvious. Brand and Deibert render obvious both limitations. Ex-1003, p. 62.

First, as discussed in [1.4], Brand discloses *activation* of the *authentication function* when the authentication application is initiated.

Second, as discussed in [2.1], Brand and Deibert teach *deactivating* the authentication application. Deibert's deactivation timer begins counting down when "the mobile phone is ready to conduct the transaction." Ex-1007, 9:35-38; *see also id.* 3:48-51.

In light of Deibert's teachings, it would have been obvious to a POSITA to start the countdown for a predetermined timeout time to deactivate Brand's authentication application after the user initiated the application. Ex-1003, p. 62. This would make the application easier to use. Starting the deactivation timer when the authentication is activated would ensure that, irrespective of the user's action or inaction, the authentication application does not remain active indefinitely. This would also free resources on the mobile device. Ex-1003, p. 62. Additionally, setting the countdown for a predetermined timeout time to deactivate the authentication application after it was activated is a simple matter of a design choice. Ex-1003, p. 62; *see* Reasons to Combine Brand and Deibert, § IX.C.5.

Accordingly, Brand and Deibert teach deactivating the authentication application after a predetermined time period that starts when the authentication application is initiated, which renders obvious "*[deactivating the authentication function after...] activation thereof*," as claimed. Ex-1003, pp. 62-63.

[2.3] *[deactivating the authentication function after at least one of ...]* when an active state thereof has been checked.

Brand and Deibert renders this limitation obvious. As discussed in [1.5], Brand's disclosure of a result transmitted from the authentication application (*authentication function*) to the authentication server teaches that the authentication application is *active*. Ex-1003, p. 63. Brand further discloses that the authentication server *checks* that the authentication application is active because the server reads the result and sends a positive or negative "authentication result" to the banking institution server. Ex-1005, 7:8-15, 7:25-29, 8:25-31; Ex-1003, p. 63.

As discussed in [1.6] and [2.2], it would have been obvious to a POSITA to use Deibert's deactivation code to deactivate Brand's authentication application after the authentication server receives a result from the authentication application. Ex-1003, p. 64. Additionally, initiating the timeout time to deactivate the authentication application after the authentication server receives the result is a simple matter of a design choice. Ex-1003, p. 64. *See* Reasons to Combine Brand and Deibert, § IX.C.5.

Accordingly, Brand and Deibert teach deactivating the authentication application after the authentication server checks the result, which renders obvious "*[deactivating the authentication function after...] when an active state thereof has been checked*." Ex-1003, p. 64.

8. Claim 3

[3.0] ***The method of claim 1,***

See analysis at [1.0]-[1.6]. Ex-1003, p. 64.

[3.1] ***wherein said authentication step includes the step of logging-on the mobile device to a mobile communications network that provides the second communication channel.***

Brand discloses this limitation. First, as discussed in [1.2], Brand discloses a communication link (*second communication channel*) in "a **GSM network**." Ex-1005, 5:65-6:3. A POSITA would have been familiar with GSM as a well-known standard for digital cellular telephones. Ex-1003, p. 65. The GSM network is the "*mobile communications network that provides the second communication channel*." Ex-1003, p. 65

Second, Brand discloses that the mobile phone "establish[es] a communication link with the authentication server" via a GPRS signal. Ex-1005, 11:6-14; 5:65-6:1. A POSITA would have understood that GPRS is a packet switched service that transmits voice and data using the GSM network's infrastructure. Ex-1003, p. 65. Accordingly, for a mobile device to establish a communication link in the GSM network with a GPRS signal, the mobile device would first need to *log[]-on* to the GSM network to access the infrastructure. Ex-1003, p. 65.

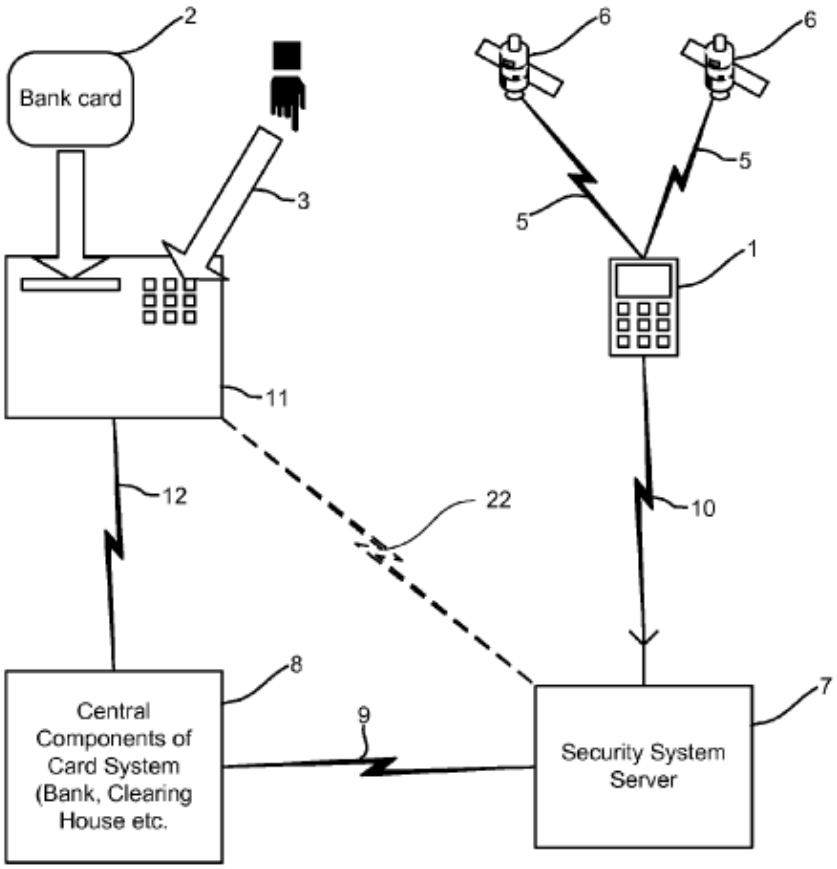
Third, as discussed in [1.2], Brand discloses *the authentication step*. Ex-1003, p. 65. Brand further discloses that the communication link is established when the authentication "application sends the digital fingerprint (13) via the network (11) by means of a GPRS protocol to the authentication server," which is during the *authentication step*. Ex-1005, 6:53-64; Ex-1003, p. 66

Accordingly, by disclosing that the mobile device establishes a communication link over a GSM network when the authentication application is initiated, Brand discloses "*wherein said authentication step includes the step of logging-on the mobile device to a mobile communications network that provides the second communication channel*." Ex-1003, p. 66.

D. Ground 2: Claims 5, 6, 7, 8, 10, and 11 are obvious over Brand, Williams, Deibert, and Carter

1. Carter

Carter generally relates to authenticating transactions with a mobile device. Ex-1008, Abstract. Carter's authentication system is illustrated in Figure 1 (below).



Ex-1008, Figure 1

Carter describes a mobile device (MS) that exchanges tokens with "server 7 of the security system that opens a time and location transaction window in which trusted payments and transaction requests can be initiated and 'passed on' to the present existing card system." Ex-1008, ¶¶ 103, 113. The security server "checks the location of the MS 1 associated with the card 2 to be authorised." Ex-1008, ¶ 120. If MS 1 "is within a predetermined distance of the terminal 11, from which the authorisation is being sought, it returns an authorisation to the card server to propose to permit the transaction." Ex-1008, ¶ 120. To determine location of the

MS, "GPS satellite system" or "GSM/UMTS, WiFi and other terrestrial radio based technology" may be used. Ex-1008, ¶¶ 104, 133-134.

2. Reasons to Combine Brand and Carter

A POSITA would have been motivated to combine the teachings of Brand's authentication system with Carter for multiple reasons, including to obtain the obvious, beneficial, and predictable result of improving the system's security. Ex-1003, ¶ 97.

As an initial matter, a POSITA when considering the teachings of Brand would have also considered the teachings of Carter, as they are analogous prior art both pertaining to the field of authenticating transactions. Ex-1005, Abstract; Ex-1008, Abstract; Ex-1003, ¶ 98.

a) Determining location of the mobile device while authenticating the transaction increases security of the authentication system.

Brand describes an authentication technique that relies on a user always being "in possession of his/her mobile phone" and "a one-to-one relationship between the digital fingerprint (13) and user." Ex-1005, 6:18-21. A POSITA would have recognized that while Brand's authentication system may still authenticate fraudulent transactions when a user mistakenly authenticates a transaction the user did not initiate. Ex-1003, ¶ 100. To prevent such occurrences, a POSITA would

have looked to techniques to further reduce the likelihood of mistaken authentications. Ex-1003, ¶ 100.

Carter's location technique would beneficially reduce instances when Brand's authentication system authenticates fraudulent transactions. Ex-1003, ¶ 100. Carter teaches that "location based security may be used to increase the security of a great many 'transactions.'" Ex-1008, ¶ 309. This is because Carter's system "can check to see if the mobile device is near to a location" from which a user conducts a transaction, *e.g.*, Brand's terminal. Ex-1008, ¶ 46. A POSITA would have recognized that Carter's system adds additional or supplements existing verifications that confirm that the user who possesses the mobile device is the same user conducting the transaction. Ex-1003, ¶ 101. Accordingly, it would have been obvious to a POSITA to implement Carter's locating technique that determines whether Brand's mobile device is proximate to the terminal from which the user conducts a transaction to make the authentication system more secure. Ex-1003, ¶ 101. Indeed, the system of Brand and Carter would prevent a user from inadvertently or mistakenly approving a transaction initiated at a terminal that is not near the user. Ex-1003, ¶ 101.

b) **Using locating techniques is a cost-effective way to increase security of the authentication system.**

A POSITA would have looked to cost-effective techniques that verified that a user possessed his mobile device. Ex-1003, ¶ 102. Brand describes cost as a factor for implementing authentication techniques. Ex-1005, 2:3-6, 2:16-18. Carter teaches existing location techniques, e.g., "a built-in or connected GPS... or other location determining capability" that the mobile device uses to determine its location. Ex-1008, ¶ 104. In this way, "no significant hardware modifications to the MS [mobile station] are needed." Ex-1008, ¶ 104. Carter further teaches that "GPS receivers are now available 'on-a-chip' and are as cheap as £8." Ex-1008, ¶ 251, *see also* ¶ 334 ("[GPS] chips have become so cheap that adding their costs to the cost of manufacturing the appliance will be weighing advantageously against the cost of losses in connection with piracy."). A POSITA looking at cost as a factor for making the authentication system more secure, would look to the teachings in Carter that determine location of the mobile device using cheap and existing techniques. Ex-1003, ¶ 102. Accordingly, it would have been obvious to a POSITA to implement existing location techniques taught in Carter in Brand's mobile device as a cost-effective way to verify that a user possesses the mobile device when the user is conducting a transaction. Ex-1003, ¶ 102.

c) **Combining location with other authentication techniques makes the authentication system more reliable.**

As discussed above, a POSITA would have found it obvious to combine the locating technique with other authentication techniques to authenticate the user. Ex-1003, ¶ 103. However, a POSITA would have recognized that locating techniques may not always be available. Ex-1003, ¶ 103. Carter describes that a GPS system has poor indoor coverage and also areas where radio networks are not available. Ex-1008, ¶¶ 137, 171. A POSITA would have recognized that in those cases the authentication system that relies on locating techniques may not be able to determine the location of the mobile device and its proximity to the terminal. Ex-1003, ¶ 103. Thus, the authentication system would not be able locate the user and might, therefore, deny the requested transaction. Ex-1003, ¶ 103.

It would have been obvious to a POSITA that in such circumstances, the authentication system would rely on other techniques to authenticate the user to the transaction. Ex-1003, ¶ 104. Carter confirms this, stating that "known identity verification methods may prove useful in combination with other security systems features" when the locating technique is not available. Ex-1008, ¶ 171. Carter explains that this would "allow[] the security system to continue to validate the authenticity of a transaction based on these further identifying criteria, rather than necessarily geographical proximity." Ex-1008, ¶ 171.

In light of Carter's teachings, it would have been obvious to a POSITA that the authentication system that authenticates the user by determining location of the mobile device would determine whether the authentication application is active when the locating technique is not working. Ex-1003, ¶¶ 105-107. This would make the authentication system more reliable because the authentication system would have another technique that it can use to authenticate a user to a transaction. Ex-1003, ¶¶ 105-106. Further, the authentication system would not treat genuine transactions as fraudulent because its location technique is not working. Ex-1003, ¶¶ 105-107.

d) Increasing security of the authentication system by encrypting user information and transmitting user information over different channels.

Brand describes a way to "authenticat[e] the identity of users conducting secure transactions" is to verify user information, such as "a login identifier (username) and a secret password" that a user enters to gain access to a program or website. Ex-1005, 1:6-8, 1:18-20; *see also id.* 6:47-55. Brand describes spyware, such as "key-logging" software that can be "secretly installed by criminals on computers" and allow "a third party to secretly record a user's login identifier and password and use them at a later stage to gain unauthorized access to the user's secure information." Ex-1005, 1:41-49. Brand also describes that encrypting data "effectively prevents so-called 'man-in-the-middle' attacks." Ex-1005, 10:20-21. A

POSITA would have recognized that encrypting a password during transmission does not protect it from being illicitly obtained via key-logging software. Ex-1003, ¶ 108. Accordingly, a POSITA would have recognized that techniques that protect user's information are desirable because they prevent a third-party from stealing the information. Ex-1003, ¶ 108.

First, Carter teaches that "improved security can be obtained when the payment data is split over two independent terminal stations and sent over two independent communication networks instead of one." Ex-1008, ¶ 147. Carter teaches that "it is possible to use the MS as the 'terminal'" that sends the PIN portion of the payment transaction while the rest of the user information is entered at the terminal. Ex-1008, ¶¶ 148-149. Carter explains that sending the PIN over MS makes "it harder for criminals to see what the PIN is, providing a further level of security." Ex-1008, ¶ 149.

It would have been obvious to a POSITA, in view of Carter's teachings, to modify Brand's system such that the user would enter a password using the mobile device instead of the terminal. Ex-1003, ¶ 110. This would make Brand's authentication system more secure by bifurcating user's information over different electronic devices and transmitting it over different channels. Ex-1003, ¶ 110. In this way, a third-party using spyware installed on a computer to observe a user

logging into the banking website would not learn the user's password because the user entered the password using the mobile device. Ex-1003, ¶ 110.

Such a modification is simply the combination combining prior art elements (entering Brand's user account and password using different terminals and transmitting them over different channels as taught in Carter) according to known methods (bifurcating login information across multiple devices) to yield predictable results (protecting information). Ex-1003, ¶ 111. A POSITA would have been readily able to predict the result of such a combination because sending the password separately is "a user friendly security feature" that does not unduly burden the authentication process. Ex-1008, ¶ 147; Ex-1003, ¶ 111.

Second, Carter teaches that "the wireless communication means are adapted to establish communication tunnels between sender and receiver comprising VPN and wherein the data transported through said tunnels is encrypted" using "cryptographic and tunnelling means." Ex-1008, ¶¶ 86-87. Carter further teaches that the GSM network employs "embedded security feature" including "AES (Advanced Encryption Standard) cryptography and state-of-the-art hashing methodologies." Ex-1008, ¶ 185.

It would have been obvious to a POSITA, in view of Carter's teachings, for Brand's mobile device to generate an encrypted password. Ex-1003, ¶ 113. This would make Brand's authentication system more secure because the user's

information would not be transmitted unencrypted where it is susceptible to the "man-in-the-middle" attacks. Ex-1003, ¶ 113. Further, the third-party who obtains the encrypted user information would not be able to decrypt the information. Ex-1003, ¶ 113.

Such a combination would have simply been combining prior art elements (encrypting Brand's password as taught in Carter) according to known methods (*e.g.*, AES encryption, hashing) to yield predictable results (preventing a third-party from obtaining the user's password). Ex-1003, ¶ 114. A POSITA would have been readily able to predict the result of such a combination because Carter describes the result of its techniques and because a GSM system uses "embedded security features" including encryption and hashing. Carter, ¶ 185. Because encrypting wireless data was known in the art, such a combination would have been within the skill level of the POSITA. Ex-1003, ¶ 114; Ex-1008, ¶¶ 86-87.

3. Claim 5

[5.0] ***The method of claim 1***

See analysis at [1.0]-[1.6]. Ex-1003, p. 78.

[5.1] ***further comprising the step of having the authentication device determine a current location of the mobile device and***

Brand in combination with Carter renders this limitation obvious. First, as discussed in [1.2], Brand discloses an authentication server (*authentication device*).

Second, Carter teaches a security server that "**checks the location of the MS 1** associated with the card 2 to be authorised" as the user attempts to use "the card at the terminal." Ex-1008, ¶¶ 120, 124. The MS is a mobile device. Ex-1008, ¶ 103. The location of the MS as the user uses "the card at the terminal" is *a current location*. Ex-1008, ¶ 124; Ex-1003, pp. 78-79.

It would have been obvious to a POSITA for Brand's authentication server to determine the location of the mobile device as taught in Carter to make the authentication system more secure by determining whether the location of the mobile device is proximate to the terminal where the user is conducting a transaction. Ex-1003, p. 79. This in turn would indicate whether the user initiating the transaction possesses the mobile device. Ex-1003, p. 79. *See* Reasons to Combine Brand and Carter, § IX.D.2.a.

Accordingly, Brand and Carter teach an authentication server that determines the location of the mobile device, which renders obvious this limitation. Ex-1003, p. 79.

[5.2] ***denying the authentication of the user when the locations of the terminal and of the mobile device do not fulfil a predetermined spatial relationship.***

Brand and Carter render this limitation obvious. Carter teaches that "security server 7 checks the **location of the MS 1** associated with the card 2 to be authorised" with "respect of the location of the ... terminal." Ex-1008, ¶¶ 120, 115.

If MS 1 "is within a **predetermined distance of the terminal 11**" the security server "returns an authorisation to the card server to propose to permit the transaction to take place." Ex-1008, ¶ 120. Carter further teaches that "when the location verification fails," the security system 7 "may prevent authorisation requests from a boundary terminal 11 ever reaching the card system 8," thus *denying the authentication of the user*. Ex-1008, ¶ 115; Ex-1003, pp. 79-80. Because the verification fails when the MS is "outside of the acceptable vicinity" of the terminal, Carter teaches *locations of the terminal and of the mobile device do not fulfil a predetermined spatial relationship*. Ex-1008, ¶ 124; Ex-1003, pp. 80-81.

It would have been obvious to a POSITA that Brand's authentication server would not authenticate the user to the transaction when the user's mobile device is not within a predetermined distance from a terminal as taught in Carter. Ex-1003, p. 81. This is an indication of a fraudulent transaction, and denying the transaction would make the authentication system more secure. Ex-1003, pp. 80-81. *See* Reasons to Combine Brand and Carter, § IX.D.2.a.

Accordingly, Brand and Carter teach an authentication server that does not authenticate a transaction when the user's mobile device is not within a predetermined distance from a terminal, which renders this limitation obvious. Ex-1003, p. 81.

4. Claim 6

[6.0] ***The method according to claim 5,***

See analysis at [5.0]-[5.2]. Ex-1003, p. 81.

[6.1] ***wherein the second communication channel involves a mobile communications network supporting Location Based Services, and***

Brand and Carter render this limitation obvious. First, as discussed in [1.2], *the second communication channel* is a GSM communication link. As discussed in [3.1], the GSM network is a *mobile communication network.*

Second, Carter teaches that "**locating technologies** do exist such as **using** e.g. **GSM**/UMTS, WiFi and other terrestrial radio based **technology**." Ex-1008, ¶ 133. Because GSM provides locating technologies, a POSITA would have recognized that Brand's GSM network *support[s] Location Based Services*. Ex-1003, pp. 81-82.

It would have been obvious to a POSITA to use the GSM network's locating technologies to determine the location of Brand's mobile device to make the authentication system more secure. Ex-1003, p. 82. A POSITA would have been motivated to use cheap, existing locating technologies that are already built into the GSM network. Ex-1003, p. 82; Ex-1008, ¶¶ 251, 334. *See also* Reasons to Combine Brand and Carter, § IX.D.2.a-b.

Accordingly, Brand and Carter teach a GSM network that supports locating technologies to locate a mobile device, which renders this limitation obvious. Ex-1003, p. 82.

[6.2] ***further comprising the step of having the authentication device use these Location Based Services for locating the mobile device.***

Brand and Carter render this limitation obvious. First, as discussed in [1.2], Brand discloses an authentication server (*authentication device*).

Second, Carter teaches the security server that "checks the **location of the MS 1** associated with the card 2 to be authorised" using "the current GPS satellite system" or the locating technologies such as "GSM/UMTS, WiFi and other terrestrial radio based technology." Ex-1008, ¶¶ 120, 133, *see also id* ¶¶ 84, 124. As discussed in [6.1], locating technologies provided by a GSM network are the *Location Based Services*. Ex-1003, pp. 82-83.

It would have been obvious to a POSITA for Brand's authentication server to determine the location of the mobile device using the GSM network's locating technologies to make the authentication system more secure. Ex-1003, pp. 83-84; Ex-1008, ¶¶ 251, 334. *See* Reasons to Combine Brand and Carter, § IX.D.2.a-b.

Accordingly, Brand and Carter teach the authentication server that uses locating technologies to locate a mobile station, which renders this limitation obvious. Ex-1003, p. 84.

5. Claim 7

[7.0] The method according to claim 5,

See analysis at [5.0]-[5.2]. Ex-1003, p. 84.

[7.1] further comprising the step of having the mobile device detect its own location and

Brand and Carter render this limitation obvious. First, as discussed in [1.2], Brand discloses a *mobile device*.

Second, Carter teaches "[a] standard **cellular phone (referred to as MS) with a built-in or connected GPS or equivalent receiver (or other location determining capability**)." Ex-1008, ¶ 104; *see also* Ex-1008, ¶ 91 ("**the location determining means of the mobile device** comprises electronic direction finding means comprising compass, gyroscope or pedometer."). A POSITA would have recognized that a *mobile device* with location determining capability would *detect its own location*. Ex-1003, pp. 84-85.

It would have been obvious to a POSITA for Brand's mobile device to use built-in locating technologies described in Carter because it would make the authentication system more secure. Ex-1003, p. 85. It would also be a cost-effective approach to security because mobile devices already included built-in location technologies and if they do not, the GPS receivers are cheap. Ex-1008, ¶¶ 104, 251, 334; Ex-1003, p. 85. *See* also Reasons to Combine Brand and Carter, § IX.D.2.a-b.

Accordingly, Brand and Carter teach a mobile device that has built-in locating technology that detects location this limitation. Ex-1003, p. 85.

[7.2] send location information to the authentication device.

Brand and Carter renders this limitation obvious. First, as discussed in [1.2], Brand discloses that the *mobile device* communicates with the authentication server (*authentication device*) over a GSM network.

Second, Carter teaches that "security system 7 interfaces with the MS 1 via a standard wireless communications link." Ex-1008, ¶ 120. The security system in Carter is analogous to the authentication server in Brand because both systems authenticate transactions. Ex-1005, 7:1-17, Ex-1008, ¶ 114-115; Ex-1003, p. 86. Carter further teaches that the security system takes locations "from two devices i.e. the MS and the terminal" and the "mobile device can be used to provide location information." Ex-1008, ¶¶ 52, 65. It would have been obvious to a POSITA that for the mobile station to send its location information to the security system via the wireless communication link (e.g., GSM network link) because that is the only communication path depicted in Carter between the mobile station and the security system. Ex-1008, Fig. 1; Ex-1003, p. 86.

In light of Carter's teachings, it would have been obvious to a POSITA that the mobile device would determine and transmit its location to the authentication server in Brand. Ex-1003, p. 86. Brand's authentication server already confirms (or

denies) transactions based the "result" transmitted from the mobile device. Ex-1005, 7:12-15, 7:25-29. Adding location to the transmission would make the authentication system more secure because the authentication server would be able to use the location to confirm that the mobile device is proximate to the terminal. Ex-1003, pp. 86-87. Further, the combination would to be a cost-effective way for securing the authentication system. Ex-1003, p. 87; Ex-1008, ¶¶ 251, 334. *See also* Reasons to Combine Brand and Carter, §§ IX.D.2.a-b.

Accordingly, Brand and Carter teach the authentication server that receives location information determined on the mobile device, which renders this limitation obvious. Ex-1003, p. 87.

6. Claim 8

[8.0] The method according to claim 1, further comprising the steps of:

See analysis at [1.0]-[1.6]. Ex-1003, p. 87.

[8.1] having the authentication device determine a current location of the mobile device and

See analysis at [5.1]. Ex-1003, p. 87.

[8.2] authenticate the user when the locations of the terminal and of the mobile device fulfil a predetermined spatial relationship, and

Brand and Carter render this limitation obvious. First, as discussed in [1.0], [1.2] Brand discloses authentication server (*authentication device*) that *authenticate[s] the user* to a transaction.

Second, as discussed in [5.2] Carter teaches *the locations of the terminal and of the mobile device*. Carter further teaches if MS "is within **a predetermined distance of the terminal 11**, from which the authorisation is being sought," the security server "returns an authorisation to the card server to propose to permit the transaction to take place." Ex-1008, ¶ 120. Thus, Carter teaches to *authenticate the user* to a transaction because the authorization returned to the card server allows the user to make purchases (transactions) "against the card." Ex-1008, ¶ 124; Ex-1003, p. 88.

It would have been obvious to a POSITA, in light of Carter's teachings, for Brand's authentication server to authenticate the user whose mobile device is within a predetermined distance from a terminal where the user conducts a transaction because it would make the authentication system more secure. Ex-1003, p. 88. For example, when a user's mobile device and the terminal are predetermined distance from each other, the user likely possesses the mobile device, which indicates that the user is the one conducting the transaction. Ex-1003, p. 88. *See also* Reasons to Combine Brand and Carter, § IX.D.2.a.

Accordingly, Brand and Carter teach an authentication server that authorizes a transaction when the user's mobile station is predetermined distance from a terminal, which renders obvious this limitation. Ex-1003, p. 89.

[8.3] checking the active state of the authentication function in the mobile device only when said spatial relationship is not fulfilled.

Brand and Carter render this limitation obvious. First, as discussed in [1.5], Brand discloses a result that indicates that the authentication application (*authentication function*) in the *mobile device* is *active*. As discussed in [2.3], Brand discloses that the authentication server *check[s] the active state* of the authentication application.

Second, as discussed in [5.2], Carter describes that the authentication fails when *the spatial relationship* between the terminal and the mobile station is *not fulfilled*. Ex-1003, p. 89.

Third, Carter describes "weaknesses of the current GPS system in terms of indoor coverage." Ex-1008, ¶¶ 166, 171. This occurs when users are within large buildings, subways, or other physical locations with limited capability to receive location information. Ex-1003, p. 90. A POSITA would have recognized that the locating techniques that depend on a GPS signal would not work in places where the signal is unavailable. Ex-1003, p. 90. In this case, the authentication system would not be able to determine geographic proximity between the mobile device and the terminal, and the *spatial relationship* would be *not fulfilled*. Ex-1003, p. 90. Carter teaches that when a signal used to determine location is not available other "known identity verification methods may prove useful... to continue to

validate the authenticity of a transaction based on these further identifying criteria, rather than necessarily geographical proximity." Ex-1008, ¶ 171.

In light of the teachings in Carter, a POSITA would have also recognized that locating techniques may not always be available. Ex-1003, p. 90; Ex-1008, ¶¶ 166-167, 171. To make the authentication system more reliable, it would have been obvious to a POSITA to employ multiple authentication techniques to authenticate the use to the transaction. Ex-1003, pp. 90-91. Checking whether the authentication application is active, as taught in Brand, is another identity verification technique that authenticates the user to the transaction. Ex-1003, 91. It would have been obvious to a POSITA to employ Brand's check of the authentication application as a backup alternative in the event that the mobile device's location cannot be determined. Ex-1003, 91. In this way, the authentication system of Brand and Carter would continue to authenticate the user to the transaction and would not frustrate the user by preventing a transaction because of the drawbacks in locating technology. Ex-1003, 91. *See also* Reasons to Combine Brand and Carter, § IX.D.2.c.

Accordingly, Brand and Carter teach that if the authentication server relying on locating technology is unable to determine the geographic proximity between the mobile device and the terminal, the authentication server would check a result

that indicates that the authentication application is in an active state, which renders this limitation obvious. Ex-1003, p. 91.

7. Claim 10

[10.0] The method according to claim 1,

See analysis at [1.0]-[1.6]. Ex-1003, p. 91.

[10.1] further comprising the step of transmitting a password to the transaction partner via the authentication device.

Brand and Carter render this limitation obvious. First, as discussed in [1.1], Brand discloses a banking institution (*transaction partner*) and as discussed in [1.2], an authentication server (*authentication device*.)

Second, Carter teaches that the mobile device "sends e.g. **PIN** Code and withdrawal amount to the clearing agent using another communication network 10" which is connected to the security system. Ex-1008, ¶ 148. "**[T]he security system can send** these data in a strong hash encrypted format so that the **four digit PIN** and the amount is not human readable and only understood by the processing **clearing agent**" or "**bank**." Ex-1008, ¶¶ 148, 119, *see* Figure. 1.

A POSITA would have recognized that Brand's banking institution is analogous to Carter's bank, that Brand's authentication server is analogous to Carter's security system, and that Brand's password is analogous to Carter's PIN code. Ex-1003, p. 93.

It would have been obvious to a POSITA to transmit the user account number and user password using different communication networks, as taught in Carter, to make Brand's authentication system more secure. Ex-1003, p. 93. This is because the system transmits the password by a mobile device and separately from a terminal that transmits the account number. Ex-1003, p. 93. This thwarts spyware attacks that seek to capture a user's login credentials by recording the user's keystrokes entered at a terminal. Ex-1003, p. 93; Ex-1005, 1:41-49. When the user account and password entered and transmitted using different devices and channels, it is harder for the unauthorized third-party to steal both the account number and the password. Ex-1003, pp. 93-94. It would have been obvious to a POSITA for the user's mobile phone to transmit the user's password to the banking institution via the authentication server because, as shown in Brand's Fig. 1, that is the only communication path established between the mobile phone and the banking institution. *See also* Reasons to Combine Brand and Carter, § IX.D.2.d.

Accordingly, Brand and Carter teach an authentication server that receives a password from a mobile device and sends the password to the banking institution, which renders this limitation obvious. Ex-1003, p. 94

8. Claim 11

[11.0] The method according to claim 10, further comprising

See analysis at [10.0]-[10.1]. Ex-1003, p. 94.

[11.1] the steps of one of storing and generating the password in the mobile device and transmitting the password to the authentication device.

As discussed regarding claim construction, this limitation requires either (1) *storing* and *transmitting the password* or (2) *generating* and *transmitting the password*. Brand and Carter render obvious the "*generating*" and "*transmitting*" steps. Ex-1003, p. 94.

First, as discussed in [10.1], Carter teaches "*transmitting the password to the authentication device.*" Ex-1003, p. 94.

Second, Carter teaches that "**information or data to and from the mobile device**, required to authenticate, identify, validate,... or determine is concealed using **cryptographic and data tunnelling means**," such as AES cryptography and hashing. Ex-1008, ¶¶ 86-87. Since the user in Carter "enter[s] the PIN on the MS" and the mobile device "**sends** e.g. **PIN** Code," the mobile device in Carter encrypts (*generate[s]*) the PIN Code before the encrypted PIN Code is transmitted through the tunnel. Ex-1008, ¶ 148.

It would have been obvious to a POSITA to encrypt the password using Carter's encryption techniques to securely transmit the password over a GSM network. Ex-1003, p. 95. Confirming this, Carter teaches that "embedded security features" including AES cryptography and hashing, were included in the

"GSM/UMTS network" and were known to a POSITA. Ex-1003, pp. 95-96. *See also* Reasons to Combine Brand and Carter, § IX.D.2.d.

Accordingly, Brand and Carter teach a mobile device that encrypts a password and sends the encrypted password to the authentication server, which renders obvious this limitation. Ex-1003, p. 96.

E. Ground 3: Claims 11 and 12 are obvious over Brand, Williams, Deibert, Carter, and Nielsen.

1. Nielsen

Nielsen generally relates to "a system for managing password access to a plurality of remote servers, such as remote web sites." Ex-1009, 3:53-55. Nielsen teaches a password management system that "maintains a database of passwords and user IDs as they are known to the remote sites." Ex-1009, 3:67-4:2. "At least the password, and... the user ID are encrypted using a master password." Ex-1009, 4:21-23. Nielsen teaches that "[w]hen a request for authentication is received," the password management system "intercepts the request,... decrypts the needed password and user ID using the master password." Ex-1009, 4:3-8. The password management system then "forwards the decrypted password and user ID to the requesting remote site." Ex-1009, 4:7-8.

2. Reasons to Combine Brand and Carter with Nielsen

A POSITA would have been motivated to combine the teachings of Brand and Carter with Nielsen for multiple reasons, including the obvious, beneficial, and predictable result for making the authentication system easier to use. Ex-1003, ¶ 118.

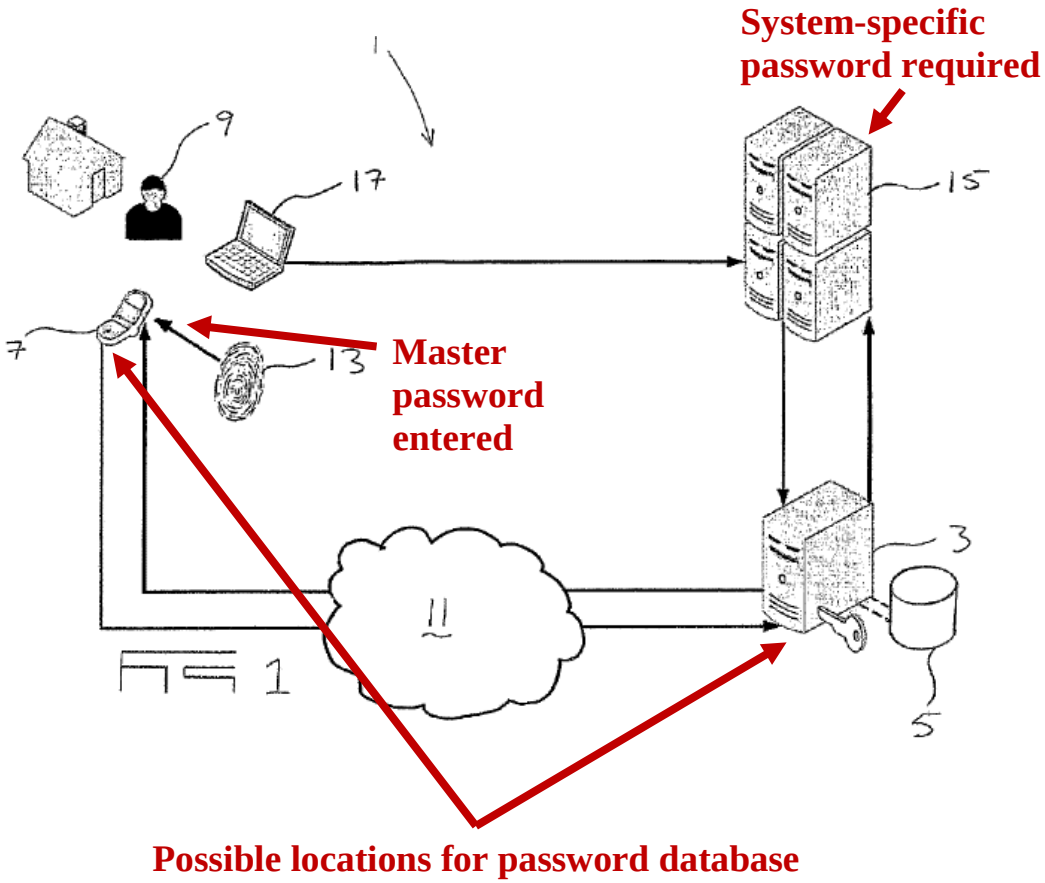
First, a POSITA considering the teachings of Brand and Carter would have also considered the teachings of Nielsen, as they are analogous prior art pertaining to the field of authentication. Ex-1005, Abstract; Ex-1008, Abstract; Ex-1009, Abstract; Ex-1003, ¶ 119.

Second, the combination of Brand and Carter teaches a user password that is transmitted to a transaction partner via an authentication server. Ex-1003, ¶ 120. A POSITA would have recognized that in this system, a user accessing multiple transaction partners would need to remember multiple passwords to initiate the authentication process for each transaction partner. Ex-1003, ¶ 120. Remembering multiple passwords would make the log-in process difficult for the user. Ex-1003, ¶ 120. Some users would respond by reusing passwords or using an easy-to-guess password. Ex-1003, ¶ 120. A POSITA would have recognized that such passwords are weak and risk being discovered by unauthorized individuals. Ex-1009, 1:24-26; 1005, 1:41-49; Ex-1003, ¶ 120.

Nielsen teaches "a single master password that will be used to access many remote servers." Ex-1009, 3:64-67. The master password encrypts "passwords and user IDs for remote servers to which the user is registered." Ex-1009, 1:65-2:1, *see also* 3:67-4:3.

It would have been obvious to a POSITA, in view of Nielsen's teachings, to employ a password database in the system of Brand and Carter because it would make the system easier to use. Ex-1003, ¶ 122. A user would need to remember only a single master password to log into multiple transaction partners, *e.g.*, banking institutions or other websites. Nielsen explains that since "only the master password need be remembered," the master password, and "the passwords particular to specific remote sites may be made more random and thus more secure." Ex-1009, 2:1-4; Ex-1003, ¶ 122.

In modifying the system of Brand and Carter to include a password database like that in Nielsen, a POSITA would have recognized that the user would enter a master password using the mobile device, and that a system-specific password would need to be provided to the transaction partner. Ex-1003, ¶ 123. Thus, the password database would need to be located at either the mobile device or at the authentication server located on the communication path between the mobile device and the transaction partner:



Ex-1005, FIG. 1 (annotated); Ex-1003, ¶ 123.

As there are only two options for where to locate the password database, a POSITA would have found it obvious to pursue both options. *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 402 (2007). The first option, the user's mobile device, is similar to the client system in Nielsen, as they each represent devices directly used by the end user. Ex-1009, Abstract. Thus, it would have been obvious to a POSITA to employ a password database on the mobile device itself. Ex-1003, ¶

124. This would allow the user to personally exercise control over access to the database. Ex-1003, ¶ 124.

Alternatively, a POSITA would have recognized that the password database could be located at Brand's authentication server. This would allow the password database to be stored on a "fixed disk drive," as preferred in Nielsen. Ex-1009, 4:27-28; Ex-1003, ¶ 125. Storing the password database on Brand's authentication server would also prevent the database from being lost or compromised if the user's mobile phone is lost, damaged, or stolen. Ex-1003, ¶ 125.

Thus, a POSITA would have recognized that there are advantages to modifying either Brand's mobile device or Brand's authentication server to include a password database like that described in Nielsen. Ex-1003, ¶ 126.

Any modification to the system of Brand and Carter would have been within a level of one of ordinary skill in the art because the master password system that encrypts and decrypts user passwords can be implemented using "any number of computer programming languages, such as Java scripting language, 'C', Pascal, FORTRAN, assembly language, etc." Ex-1009, 6:66-7:1; Ex-1003, ¶ 127.

3. Claim 11

[11.0] The method according to claim 10, further comprising

See analysis at [10.0]-[10.1]. Ex-1003, p. 101.

[11.1] the steps of one of storing and generating the password in the mobile device and transmitting the password to the authentication device.

As discussed regarding claim construction, this limitation requires either (1) *storing* and *transmitting the password* or (2) *generating* and *transmitting the password*. Brand, Carter, and Neilson render obvious the *storing* and *transmitting*. Ex-1003, p. 101.

First, as discussed in [10.1] and in [11.1] for Ground #2, the prior art teaches *transmitting the password to the authentication device.* Ex-1003, p. 101.

Second, Neilson teaches a password management system that "maintains a database of passwords... as they are known to the remote sites." Ex-1009, 3:67-4:2. It would have been obvious to a POSITA that a database of passwords is used for *storing the password*. Ex-1003, p. 101.

In light of Nielsen's teachings, it would have been obvious to a POSITA to use a password management system in the system of Brand and Carter to make the authentication system easier to use because the user would need to remember a single master password. Ex-1003, p. 101. *See also* Reasons to Combine Brand, Carter, and Neilson, § IX.E.2.

Accordingly, Brand and Carter combined with Nielsen teach a mobile device that stores encrypted passwords which are decrypted by a master password, which

renders obvious "*storing… the password in the mobile device and transmitting the password to the authentication device*." Ex-1003, p. 102.

4. Claim 12

[12.0] The method according to claim 10, further comprising

See analysis at [10.0]-[10.1]. Ex-1003, p. 102.

[12.1] the step of one of storing and converting the password in the authentication device.

Brand, Carter, and Nielsen render this limitation obvious. As discussed above regarding claim construction, this limitation recites "*storing*" and "*converting*" as alternatives. A showing of either feature in the prior art renders this limitation obvious. Brand and Carter combined with Nielsen teach both limitations. Ex-1003, ¶ p. 102.

First, as discussed in [1.2], Brand teaches an authentication server (*authentication device*).

Second, as discussed in [11.1] in Ground #3, Neilson teaches a password management system that "maintains a database of passwords... as they are known to the remote sites." Ex-1009, 3:67-4:2. Maintaining passwords in a database including *storing* passwords.

Third, Neilson teaches that the passwords and user IDs are "encrypted using the master password." Ex-1009, 4:3. Once the "request for authentication is received, the system... decrypts the needed password and user ID using the master

password." Ex-1009, 4:3-7. A POSITA would have recognized that decrypting a needed password using a master password is *converting* the master password to a different password. Ex-1003, p. 103; *cf.* Ex-1001, 10:24-25 ("…converts the universal password into a specific password…").

In light of Nielsen's teachings, it would have been obvious to a POSITA to use the password management system in the authentication server taught in Brand and Carter. Ex-1003, p. 103. The combination would make the system easier to use because a user would remember one master password (and not multiple passwords) to access different transaction partners. Ex-1003, p. 103. *See also* Reasons to Combine Brand, Carter, and Neilson, § IX.E.2.

Accordingly, Brand and Carter combined with Nielsen teach an authentication server that stores encrypted passwords which are decrypted by a master password, which renders obvious "*the step of one of storing and converting the password in the authentication device*." Ex-1003, p. 104.

F. Ground 4: Claim 13 is obvious over Brand, Williams, Deibert, Dietrich.

1. Summary of Dietrich

Dietrich relates generally to user authentication. Ex-1023, 2:3-12. Dietrich teaches "a user computer system" which can be "a mobile telecommunication appliance, particularly a smart phone." Ex-1023, 9:28-33. "The user computer

system 100 has an interface 104 for communication with an ID token 106 which has an appropriate interface 108." Ex-1023, 9:33-36. "The ID token 106 has... protected memory area." Ex-1023, 10:7-8. The memory area stores "attributes... of the user 102, such as his name, place of residence, date of birth, sex, and/or attributes which relate to the ID token itself." Ex-1023, 10:19-26. Dietrich teaches "reading... attributes stored in the protected memory area." Ex-1023, 16:25-27.

2. Reasons to Combine Brand and Dietrich

A POSITA would have found it obvious to combine the teachings of Brand with Dietrich for multiple reasons, including to obtain the beneficial and predictable result of making the authentication system more secure. Ex-1003, ¶ 133.

First, a POSITA when considering the teachings of Brand would have also considered the teachings of Dietrich, as they are analogous prior art pertaining to the field of authentication. Ex-1005, Abstract; Ex-1023, 2:3-12; Ex-1003, ¶ 134. Dietrich's tokens were commonly used for multi-factor authentication in financial transactions, such as those in Brand. Ex-1015, Abstract, 3:15-16, 6:40-44; Ex-1005, 6:36-42. Moreover, both address methods of using mobile devices as authentication devices within a multifactor system. Ex-1003, ¶ 135.

Second, Brand teaches identity data, such as a fingerprint that the authentication application uses to log into "the authentication platform" and

establish a "real-time communication link ... between the authentication server (3)" and the mobile phone." Ex-1005, 6:55-64. Brand teaches that there is "a one-to-one relationship between the digital fingerprint (13)" used by the authentication application "and the user (9)." Ex-1005, 6:18-22. Because the authentication application uses the fingerprint to establish access to the authentication application, a POSITA would have recognized that safeguarding the fingerprint is desirable. Ex-1003, ¶ 136. Brand teaches that it is "essential that the phone's fingerprint be kept in a secure storage location," such as a "location on the phone where the phone's operating system only will allow the authentication application... to access and change it." Ex-1005, 9:7-13. Storing the fingerprint on the mobile device, however, does not safeguard the fingerprint from being stolen with the mobile device. Ex-1003, ¶ 137. Brand' solution to phone theft is for the user "to report it to the authentication service provider" to block a third party from using the fingerprint to access the authentication server. Ex-1005, 10:33-37. A POSITA would have recognized that in the interim period – i.e. from the time the user's mobile phone is stolen to the time that the user reports it to the authentication server provider, a third party may access the authentication application and attempt to authenticate transactions. Ex-1003, ¶ 137.

Dietrich teaches an identity token with a protected memory area that stores user identity attributes "such as his name, place of residence, date of birth, sex,

and/or attributes which relate to the ID token itself." Ex-1023, 10:21-26. Dietrich further teaches that "attributes are read from the protected memory area" of the identity token interfacing with the mobile device and are transmitted using an "end-to-end encryption" technique. Ex-1023, 16:16-18; 16:30-17:2.

In view of Dietrich's teachings, it would have been obvious to a POSITA to store the fingerprint taught in Brand securely within an identity token that interfaces with a mobile device. Ex-1003, ¶ 139. Storing the fingerprint in an identity token allows a user to securely store the fingerprint and safeguard the fingerprint separately from the user's mobile phone. Ex-1003, ¶ 139. In this way, even if a third party steals the user's mobile phone, the third party will not able to access the authentication application and the authentication server to authenticate transactions. Ex-1003, ¶ 139.

Third, the obviousness of incorporating Dietrich's identity token into Brand's authentication system is further evidenced by work of other artisans who incorporated the tokens into similar authentication systems to securely store data. Ex-1003, ¶ 140. Ex-1015, 3:15-16, 6:58-7:2. Because skilled artisans were incorporating identity tokens into authentication systems, a POSITA would have found it obvious to include Dietrich's identity token into Brand's authentication system. Ex-1003, ¶ 140.

3. Claim 13

[13.0] The method according to claim 1, further comprising the steps of:

See analysis at [1.0]-[1.6]. Ex-1003, p. 108.

[13.1] interfacing the mobile device to an identity token of the user to read identity data therefrom, and

Brand and Dietrich render this limitation obvious. First, as discussed in [1.2], Brand discloses a *mobile device*. Brand further a "unique digital fingerprint." Ex-1005, 6:4. The fingerprint is *identity data* because it is "uniquely associated with the specific mobile phone" of the user and identifies the mobile phone to "the authentication platform." Ex-1005, 6:5-6, 6:55-64. Ex-1003, pp. 108-109.

Second, like Brand, Dietrich also teaches a user computer system that may be "a *mobile* telecommunication appliance." Ex-1023, 9:28-32. The user computer system "has an **interface 104** for communication with an **ID token 106** which has an **appropriate interface 108**." Ex-1023, 9:33-36. The communication using interfaces 104, 108 teaches *interfacing the mobile device to an identity token*. Ex-1003, pp. 109-110.

Third, Dietrich teaches that "ID token 106 has... protected memory areas." Ex-1023, 5:15-16. The protected memory area "is used for **storing attributes**... **of the user** 102, such as his name, place of residence, date of birth, sex, and/or attributes which relate to the ID token itself." Ex-1023, 10:19-26. Dietrich explains that "the interface 104 of the user computer system 100 may be in the form of an

RFID reader" which is used to *read* "the desired attributes... from the protected memory area." Ex-1023, 21:15-17, 25:20-24.

It would have been obvious to a POSITA for the identity data, *e.g.*, fingerprint taught in Brand to be stored securely within an identity token as taught in Dietrich. Ex-1003, p. 111. Storing the fingerprint in the identity token secures the fingerprint from being stolen with the mobile device. Ex-1003, p. 111. Also, interfacing the identity token with the mobile device allows the user to securely store the fingerprint outside of the mobile device and use the mobile device to transmit the fingerprint to the authentication server. Ex-1003, p. 111; *See also* Reasons to Combine Brand and Dietrich, § IX.F.2.

Accordingly, the combination of Brand and Dietrich teaches an identity token that has an interface with a mobile device that reads the fingerprint from the token, which renders obvious this limitation. Ex-1003, p. 111.

[13.2] transmitting these identity data to the authentication device via the second communication channel.

Brand discloses this limitation. First, discussed in [1.2], Brand discloses transmitting data from a *mobile device* to an authentication server (*authentication device*) over communication link in a GSM network (*second communication channel*). As discussed in [13.1], Brand discloses that the fingerprint is *identity data*.

Second, Brand discloses that the authentication applications "**sends the digital fingerprint (13) via the [GSM] network (11) ... to the authentication server (3)**." Ex-1005, 6:55-57, 5:67.

Accordingly, Brand discloses a mobile device that transmits the fingerprint to the authentication server over a GSM network, which renders obvious this limitation. Ex-1003, p. 112.

X. CONCLUSION

Petitioner requests institution of an *inter partes* review and cancellation of the Challenged Claims.

Respectfully submitted,

Dated: September 24, 2019

/David L. McCombs/

David L. McCombs
Lead Counsel for Petitioner
Registration No. 32,271

HAYNES AND BOONE, LLP
2323 Victory Avenue, Suite 700
Dallas, Texas 75219
Customer No. 27683

CERTIFICATE OF WORD COUNT

Pursuant to 37 C.F.R. §42.24(d), Petitioner hereby certifies, in accordance with and reliance on the word count provided by the word-processing system used to prepare this Petition, that the number of words in this paper is 13,886. Pursuant to 37 C.F.R. §42.24(d), this word count excludes the table of contents, table of authorities, mandatory notices under §42.8, certificate of service, certificate of word count, appendix of exhibits, and any claim listing.

Dated: September 24, 2019

/David L. McCombs/
David L. McCombs
Lead Counsel for Petitioner
Registration No. 32,271

CERTIFICATE OF SERVICE

The undersigned certifies that, in accordance with 37 C.F.R. §42.6(e) and 37 C.F.R. §42.105, service was made on Patent Owner as detailed below.

Date of service	September 24, 2019
Manner of service	FEDERAL EXPRESS
Documents served	Petition for *Inter Partes* Review Under 35 U.S.C. § 312 and 37 C.F.R. §42.104 of U.S. 9,246,903; Exhibits 1001-1010, 1014-1015, 1020-1024; Petitioner's Power of Attorney; and Petitioner's Notice For Filing Multiple Petitions
Persons served	Richard M. Goldberg 25 East Salem Street, Suite 419 Hackensack, NJ 07601

/David L. McCombs/
David L. McCombs
Lead Counsel for Petitioner
Registration No. 32,271

EXHIBIT B

Trials@uspto.gov
571-272-7822

Paper 9
Entered: March 27, 2020

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYSTEMS, INC.,
Petitioner,

v.

MONEY AND DATA PROTECTION LIZENZ GMBH & CO. KG,
Patent Owner.

IPR2019-01638
Patent 9,246,903 B2

Before THOMAS L. GIANNETTI, BRYAN F. MOORE, and CHARLES J. BOUDREAU, *Administrative Patent Judges.*

MOORE, *Administrative Patent Judge*.

DECISION
Denying Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

A. Background

Cisco Systems, Inc. ("Petitioner" or "Cisco") filed a Petition requesting *inter partes* review of claims 1–3, 5–8, and 10–13 (the "challenged claims") of U.S. Patent No. 9,246,903 B2 (Ex. 1001, the "'903 patent"). Paper 3 ("Pet."). Money And Data Protection Lizenz GMBH & Co. KG ("Patent Owner") filed a Preliminary Response. Paper 8 ("Prelim. Resp.").

The standard for institution is set forth in 35 U.S.C. § 314, which provides that an *inter partes* review may not be instituted unless the information presented in the Petition and the Preliminary Response shows that "there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition." 35 U.S.C. § 314; *see also* 37 C.F.R § 42.4(a) ("The Board institutes the trial on behalf of the Director.").

For the reasons that follow, we do not institute *inter partes* review of the challenged claims of the '903 patent.

B. Related Proceedings

The parties identify the following pending district court proceeding involving the '903 patent: *Money and Data Protection Lizenz GmbH & Co. KG v. Duo Security, Inc.,* 1-18-cv-01477 (D. Del.). Pet. 8; Paper 7, 1.

Concurrently with the filing of this Petition, Petitioner also filed a petition challenging certain other claims of the '903 patent in IPR2019-01639. Pet. 8; Paper 7, 1. Pursuant to the Trial Practice Guide update dated July 2019, Petitioner has filed a Notice addressing the issue of multiple petitions. Paper 2.

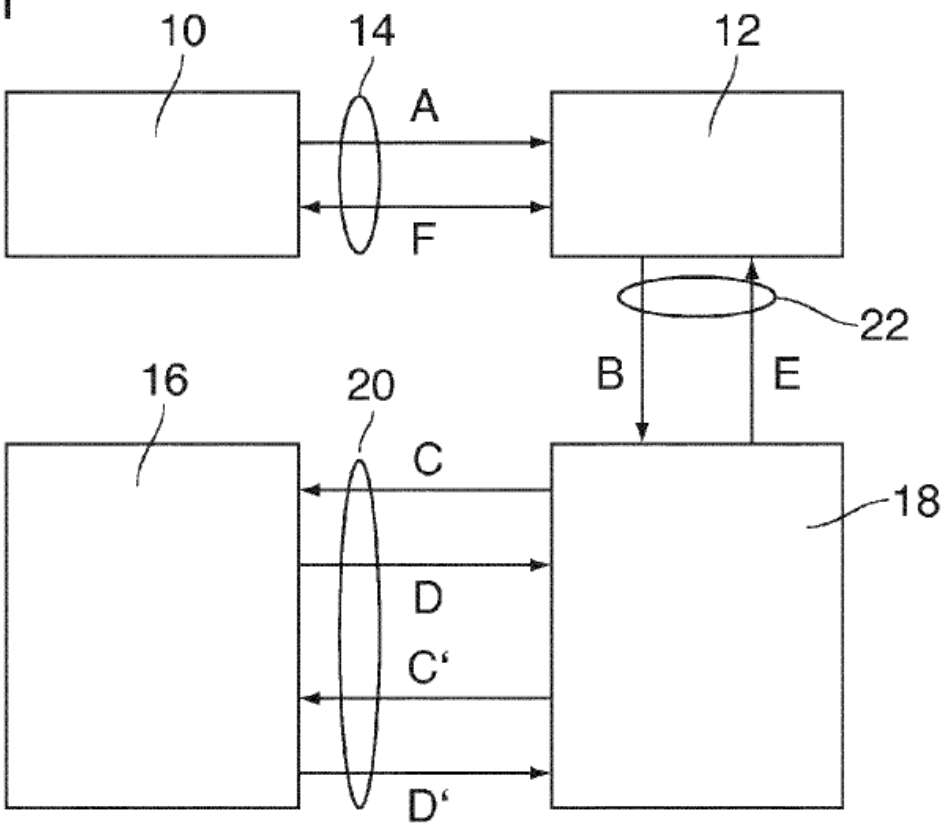
C. Real Parties in Interest

Petitioner identifies "Cisco Systems, Inc. and Duo Security, Inc." as the real parties in interest. Pet. 7. Patent Owner identifies Money and Data Protection Lizenz GmbH & Co. KG, as the real party in interest. Paper 7, 1.

D. The '903 Patent

The '903 Patent describes "authenticating a user to a transaction." Ex. 1001, 1:3–4. The authentication system includes transaction terminal 10, remote transaction partner 12, mobile communication device 16, and authentication device 18. *Id.* at 4:41–45. As illustrated in Fig. 1 below, up to three separate communication channels (14, 20, 22) link the components. *Id.* at 4:39–49.

Fig. 1



As shown in Figure 1, above, a user "operates the terminal 10 and sends a transaction request to the transaction partner 12." *Id.* at 4:57–60; FIG. 1 (A). The request includes a "user-ID." *Id.* at 4:60–61. "[T]he transaction partner 12 forwards the user-ID to the authentication device 18." *Id.* at 4:61–63, FIG. 1 (B). The "authentication device 18 retrieves the mobile telephone number and or the IMSI of the user and contacts the mobile device 16" to check whether an "authentication function . . . is active." *Id.* at 4:63–5:1, FIG. 1 (C). When the authentication device 18 confirms "that the authentication function is active, the authentication device 18 sends an authentication signal to the transaction partner 12." *Id.* at 5:1–3, FIG. 1 (D & E). The authentication signal "informs the transaction partner that this specific user is authenticated to the requested transaction." *Id.* at 5:4–7. The transaction is then "performed via the terminal 10." *Id.* at 5:7–9, FIG. 1 (F).

E. Illustrative Claims

The '903 patent has 26 claims. Eleven claims (1–3, 5–8, and 10–13) are challenged in the Petition. *See* Section I.G, *infra*. Of the challenged claims, only claim 1 is independent. Claim 1 recites:

> 1. A method of authenticating a user to a transaction at a terminal, comprising the steps of:
>
> transmitting a user identification from the terminal to a transaction partner via a first communication channel,
>
> providing an authentication step in which an authentication device uses a second communication channel for checking an authentication function that is implemented in a mobile device of the user,
>
> as a criterion for deciding whether the authentication to the transaction shall be granted or denied, having the authentication device check whether a predetermined time relation exists between the transmission of the user identification and a response from the second communication channel,

> ensuring that the authentication function is normally inactive and is activated by the user only preliminarily for the transaction,
>
> ensuring that said response from the second communication channel includes information that the authentication function is active, and
>
> thereafter ensuring that the authentication function is automatically deactivated

Ex. 1001, 10:39–60.

F. References and Other Evidence

The Petition relies on the following references:

1. US 8,862,097 B2, issued Oct. 14, 2014 (filed Dec. 3, 2009) (Ex. 1005, "Brand"),
2. GB 2,398,159 A, published Aug. 11, 2004 (Ex. 1006, "Williams"),
3. US 9,647,855 B2, issued May 9, 2017 (filed Jan. 9, 2008) (Ex. 1007, "Deibert"),
4. US 2011/0202466 A1, published Aug. 18, 2011 (Ex. 1008, "Carter")
5. US 6,182,229 B1, issued Jan. 30, 2001 (Ex. 1009, "Nielsen"), and
6. WO 2009/089943 A1, published July 23, 2009 (Ex. 1010, "Dietrich"), English translation is Ex. 1023.

Pet. 10–20.

In addition, Petitioner submits the Declaration of Patrick McDaniel (Ex. 1003, "McDaniel Decl."). Patent Owner has not submitted an expert declaration.

G. Asserted Grounds of Unpatentability

Petitioner asserts the challenged claims are unpatentable on the following grounds.

Claim(s) Challenged	Statutory Basis	References
1–3	35 U.S.C. § 103	Brand, Williams, and Deibert
5–8, 10, 11	35 U.S.C. § 103	Brand, Williams, Deibert, and Carter
11, 12	35 U.S.C. § 103	Brand, Williams, Deibert, Carter, and Nielsen
13	35 U.S.C. § 103	Brand, Williams, Deibert, and Dietrich

Pet. 14.

II. PRELIMINARY MATTERS

A. Level of Ordinary Skill

Petitioner contends:

> A Person of Ordinary Skill in The Art [] in October 2011 would have had a working knowledge of the authentication art that is pertinent to the '903 Patent, including two-factor authentication using a mobile device. A [person of ordinary skill in the art at the time of the invention] would have had a bachelor's degree in computer science, computer engineering, or an equivalent, and three years of professional experience. Lack of professional experience can be remedied by additional education, and vice versa.

Pet. 11 (citing McDaniel Decl. ¶¶ 15–19). Patent Owner contends: A person of ordinary skill in the art at the time of the invention "would have had a bachelor's degree in computer science, computer engineering, or an equivalent, and three years of work experience." Prelim. Resp. 25. Patent Owner states specifically that it is unnecessary to define the working knowledge of the person of ordinary skill in the art at the time of the invention because by definition a person of ordinary skill in the art is skilled in the art that is relevant to the '903 patent. *Id.*

We do not discern that Petitioner's statement of the "working knowledge" affects the analysis of obviousness in this decision. We do not

discern a difference between two or three years of working experience that affects the analysis of obviousness in this decision. We also regard Petitioner's definition as consistent with the prior art before us. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001) (prior art itself may reflect an appropriate level of skill). Thus, for the purpose of our decision, we adopt Petitioner's proposal.

B. Claim Construction

We interpret claim terms using "the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. 282(b)." 37 C.F.R. § 42.100(b) (2019). In this context, claim terms "are generally given their ordinary and customary meaning" as understood by a person of ordinary skill in the art in question at the time of the invention. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–13 (Fed. Cir. 2005) (citations omitted) (en banc). "In determining the meaning of the disputed claim limitation, we look principally to the intrinsic evidence of record, examining the claim language itself, the written description, and the prosecution history, if in evidence." *DePuy Spine, Inc. v. Medtronic Sofamor Danek, Inc.*, 469 F.3d 1005, 1014 (Fed. Cir. 2006) (citing *Phillips*, 415 F.3d at 1312–17). Extrinsic evidence is "less significant than the intrinsic record in determining 'the legally operative meaning of claim language.'" *Phillips*, 415 F.3d at 1317.

Petitioner requests that we construe several terms (in claims 2, 11, and 12) with language that, according to Petitioner "approximates Markush-style claiming of alternatives." *Id.* at 11–13. Patent Owner does not argue that the patentability of any claim turns on the construction for any of the above terms. *See generally* Prelim. Resp. Additionally, issues related to claim 1

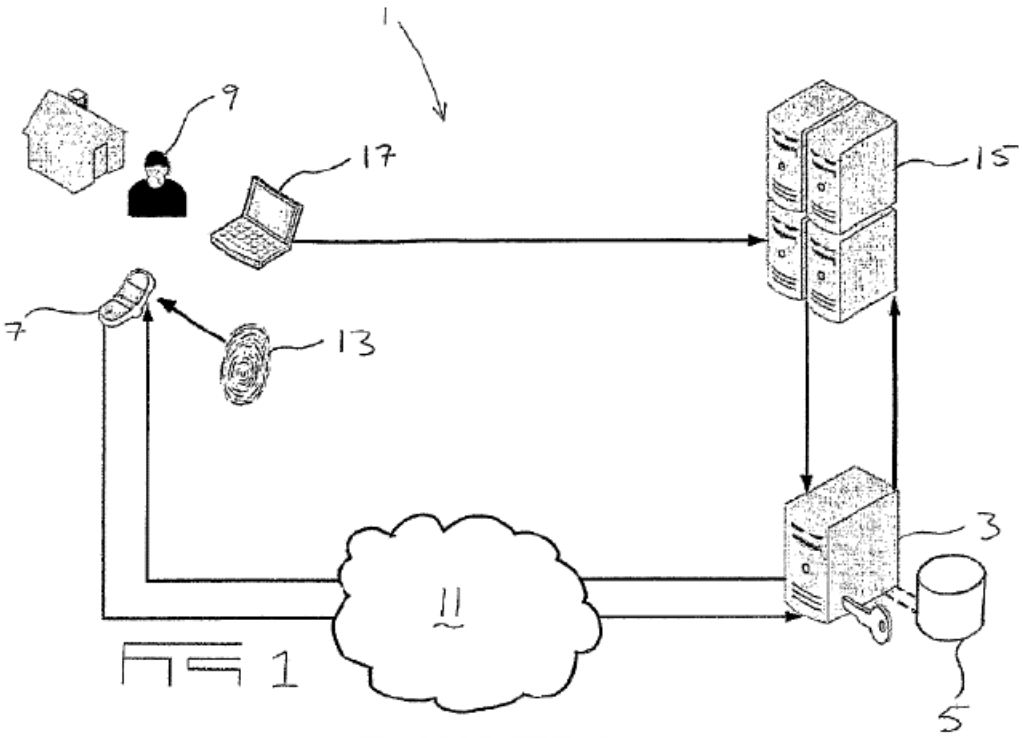
are dispositive of this decision. Thus, we see no need to construe any terms for the purposes of this decision.

C. Description of Prior Art References

Petitioner's challenge primarily relies on Brand, Williams, and Deibert. *See* Pet. 14. The remaining references (Carter, Nielsen, and Dietrich) are relied on as additional secondary references to address certain specific limitations in the dependent claims.

1. Brand (Exhibit 1005)

Brand is a patent titled "Secure Transaction Authentication." Ex. 1005, code (54). Brand discloses a system "for authenticating secure transactions between a transacting user and a secure transaction host." Ex. 1005, Abstract. Figure 1, reproduced below, shows Brand's authentication system including a user (9), user's computer (17), banking institution (15), user's mobile phone (7), and authentication server (3). Ex. 1005, 5:44, 6:48–55.



Ex-1005, FIG. 1

Figure 1 above, shows Brand's authentication system. Brand discloses that "to log into his or her internet banking account, the user (9) first accesses the website of the banking institution (15) at which his or her account is held, from a personal computer (17), laptop or other Internet enabled device." Ex. 1005, 6:47–50. The user "enters his account number (equivalent to a username) and password on the Internet banking website on his computer." Ex. 1005, 6:50–53.

"Before proceeding to login, the user (9) initiates the authentication application on his/her mobile phone." Ex. 1005, 6:53–55. The authentication application establishes a "real-time communication link" via "a GSM network" between "the authentication server" and "the mobile phone." Ex. 1005, 6:62–64, 5:67.

"Upon the user (9) requesting login to his internet banking account, the banking institution (15) requests authentication of the user (9) from the

authentication server." Ex. 1005, 7:1–3. The authentication server "sends a transaction confirmation request to the mobile phone (7) which is received by the software application." Ex. 1005, 7:3–6. The "software application triggers a pop-up on the monitor of the mobile phone" which allows "the user (9) to either confirm (accept) or deny (reject) the transaction." Ex. 1005, 7:6–12.

If the user "confirms the transaction, the application communicates this confirmation result to the server" which "sends a positive authentication result to the banking institution server." Ex. 1005, 7:12–15. The banking institution then allows the user "to proceed to its Internet banking account." Ex. 1006, 7:15–17.

2. Williams (Ex. 1006)

Williams is a patent titled "Electronic Payment Authorisation Using a Mobile Communications Device." Ex. 1006, code (54). Williams relates to "a transaction authorisation system for electronic payments." Ex. 1006, 8.[1] Williams teaches that terminals are "linked to a card issuer's central transaction processing unit." *Id.* If the amount of a transaction is above some threshold, the authorization of the transaction is suspended until it can be authorized. *Id.* at 9. The transaction processing unit has an authorization module which causes a message generation module to transmit "a SMS message identifying the card account, the transaction data and time, the merchant and the transaction value" to "a mobile communication device. . . for the card account." *Id*. The account holder "sends a return SMS message . . . using his mobile device." *Id.* at 10. If the "return SMS

[1] This decision cites to the original page numbers not the page numbers added to the Exhibit.

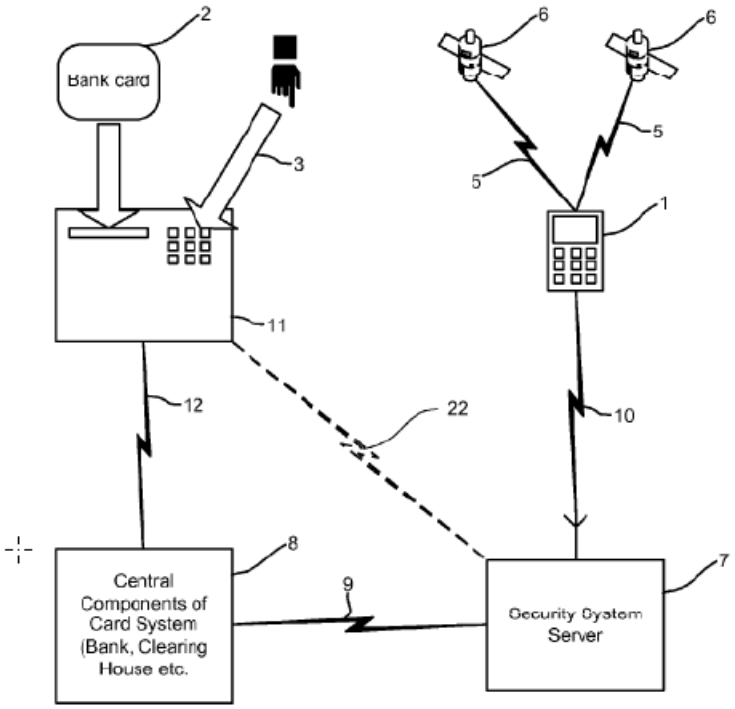
message is received within a predetermined period of time, the authorisation module 3 instructs the transaction processing unit 2 to authorise the transaction." *Id.* at 11.

3. Deibert (Ex. 1007)

Deibert is a patent titled "Mobile Phone Payment with Disabling Feature." Ex. 1007, code (54). Deibert relates to "contactless" mobile device payments. *Id*. at Abstract. Deibert describes mobile payment applications which allow wireless transmission of data allowing a payment transaction. *Id*. at 6:45–48. In Deibert, the user authenticates himself by providing a single authentication factor (i.e., "entering a password into the mobile phone application, in order to authenticate the consumer 30 and prevent fraud." (*id*. at 9:28–30)). If authentication is successful, the user's mobile phone executes a payment application "that stores payment details, such as a credit card number and related information." *Id*. at 2:49–51. For example, when a user wishes to make a purchase, he places his mobile phone "in proximity to an access device associated with the merchant. The mobile payment application may then send the payment details to the access device over a wireless connection." *Id*. at 2:51–55. Deibert also discloses that when the mobile phone is ready to conduct a transaction, the phone begins counting down from a predetermined timeout time. *Id*. at 9:30–38. If no payment transaction occurs before the timeout time elapses, the mobile payment application is disabled or deactivated. *Id*. at 9:38–40. Thus, Deibert includes "a timer that automatically deactivates any mobile payment application[] after a predetermined timeout time has elapsed." *Id*. at 6:50–52.

4. Carter (Exhibit 1008)

Carter is a patent titled "Multifactor Authentication." Ex. 1008, code (54). Carter generally relates to authenticating transactions with a mobile device. *Id.* at Abstract. Carter's authentication system is illustrated in Figure 1, reproduced below.



Ex-1008, Figure 1

Carter's authentication system is illustrated in Figure 1, above. Carter describes a mobile device (MS) that exchanges tokens with "server 7 of the security system that opens a time and location transaction window in which trusted payments and transaction requests can be initiated and 'passed on' to the present existing card system." *Id.* ¶¶ 103, 113. The security server "checks the location of the MS 1 associated with the card 2 to be authorised." *Id.* ¶ 120. If MS 1 "is within a predetermined distance of the terminal 11, from which the authorisation is being sought, it returns an authorisation to the card server to propose to permit the transaction." *Id.*

¶ 120. To determine location of the MS, "GPS satellite system" or "GSM/UMTS, WiFi and other terrestrial radio based technology" may be used. *Id.* ¶¶ 104, 133–134.

5. Nielsen (Exhibit 1009)

Nielsen is a patent titled "Password Helper Using a Client-Side Master Password Which Automatically Presents the Appropriate Server-Side Password in a Particular Remote Server." Ex. 1009, code (54). Nielsen generally relates to "a system for managing password access to a plurality of remote servers such as remote web sites." *Id.* at 3:53–55. Nielsen teaches a password management system that "maintains a database of passwords and user IDs as they are known to the remote sites." *Id.* at 3:67–4:2. "At least the password, and . . . the user ID are encrypted using a master password." *Id*. at 4:21–23. Nielsen teaches that "[w]hen a request for authentication is received," the password management system "intercepts the request, . . . decrypts the needed password and user ID using the master password, and forwards the decrypted password and user ID to the requesting remote site." *Id.* at 4:3–8.

6. Dietrich (Exhibit 1023 (English Translation))

Dietrich is a patent titled "Method for Reading Attributes from an ID Token." Ex. 1023, code (54). Dietrich relates generally to user authentication. *Id.* at 2:3–12. Dietrich teaches "a user computer system" which can be "a mobile telecommunication appliance, particularly a smart phone." *Id.* at 9:28–33. "The user computer system 100 has an interface 104 for communication with an ID token 106 which has an appropriate interface 108." *Id.* at 9:33–36. "The ID token 106 has . . . protected memory area." Ex. 1023, 10:7–8. The memory area stores "attributes... of the user 102, such as his name, place of residence, date of birth, sex, and/or

attributes which relate to the ID token itself." *Id.* at 10:19–26. Dietrich teaches "reading . . . attributes stored in the protected memory area." *Id.* at 16:25–27.

III. ANALYSIS OF THE CHALLENGED CLAIMS

A. Obviousness

A claim is unpatentable under 35 U.S.C. § 103(a) if the differences between the claimed subject matter and the prior art are such that the subject matter, as a whole, would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations, including (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in the art; and (4) where in evidence, so-called "secondary considerations," including commercial success, long-felt but unsolved needs, failure of others, and unexpected results. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966) ("the *Graham* factors").

B. Challenge to Claims 1–3 based on Brand, Williams, and Deibert

Petitioner contends these claims would have been obvious over the combination of Brand, Williams, and Deibert. Pet. 15–44. Petitioner supports this assertion with testimony from its expert, Dr. McDaniel. McDaniel Decl. ¶¶ 75–93.

1. Rationale to Combine

a. Brand and Deibert

Petitioner also argues that a person of ordinary skill would have been motivated to combine Brand and Deibert. Pet. 21–24. Petitioner contends that both Brand and Deibert describe authentication features that prevent

fraud. Pet. 21 (citing McDaniel Decl. ¶ 84; Ex. 1005, Abstract; Ex. 1007, 9:27–30). Petitioner asserts that after Brand initiates an authentication application, a person of ordinary skill in the art at the time of the invention would have known that the application continues until the phone loses power or the application is deactivated. *Id.* (citing McDaniel Decl. ¶ 84; Ex. 1005, 6:53–54). Thus, according to Petitioner, a person of ordinary skill in the art at the time of the invention would recognize automatically deactivating an authentication application would be desirable. *Id.* (citing McDaniel Decl. ¶ 85). In other words, Petitioner suggests deactivating the application would save battery life.

According to Petitioner, "Deibert teaches software 'code relating to a timer that automatically deactivates any mobile payment applications after a predetermined timeout time has elapsed.'" Pet. 22 (quoting Ex. 1007, 6:49–53). Petitioner contends that adding Deibert's automatic deactivation feature to Brand would make Brand's application easier to use than with manual deactivation and would also increase security because the user would otherwise have to reinitialize the application with the user's credentials if it deactivates. *Id.* (citing McDaniel Decl. ¶¶ 86–89). Petitioner also asserts a person of ordinary skill in the art at the time of the invention would recognize the predetermined time would start either when the authentication application is initiated or when the requested transaction is confirmed or denied. *Id.* (citing McDaniel Decl. ¶ 90).

Petitioner further contends a person of ordinary skill in the art at the time of the invention would have had a reasonable expectation of success in making the combination. *Id.* at 24. Petitioner asserts a [person of ordinary skill in the art at the time of the invention] would have been familiar with conventional coding languages in order to code the combination and thus the

"combination is simply combining prior art elements (Deibert's timer that automatically deactivates Brand's authentication application) according to known methods (code written in a programming language) to yield predictable results (automatically deactivating the authentication application)." *Id.* at 24 (citing McDaniel Decl. ¶ 91). Petitioner supports these assertions with testimony from Dr. McDaniel. *See* McDaniel Decl. ¶¶ 83–91.

Patent Owner responds that a person of ordinary skill in the art at the time of the invention would not have added Deibert's automatic deactivation to Brand. Prelim. Resp. 39. Specifically, Patent Owner argues that deactivation and the necessary associated reinitialization would frustrate both Brand's purpose of allowing multiple transactions in one session and Deibert's purpose to allow the user to interact with the system by logging on only once. *Id.* at 41–42 (citing Ex. 1005, 7:18–24; Ex. 1007, 9:45–53). Patent Owner further argues that adding such a feature could deactivate the pop-up notification of Brand and prevent the user from manually confirming or denying a transaction. *Id.* at 39.

Patent Owner relies on Brand's statement that a session can last though subsequent transactions (i.e., continuous and ongoing) depending on "the type of transaction that the user (9) attempts to perform and the decision of the bank on how to implement the security layer provided by the invention." *Id.* at 41–42 (citing Ex. 1005, 7:21–24). Therefore, Patent Owner suggests, the intent in Brand is to allow an open session with multiple transactions. *Id.*

Patent Owner further argues that Brand and Deibert are directed to "completely different aspects of a payment system" because, among other things, Brand is directed to a two-factor authentication system, whereas

Deibert is directed to a one-factor authentication system. Prelim. Resp. 40. Additionally, Patent Owner argues that Petitioner's asserted motivations of increasing security and making the system easier to use are inconsistent with each other because additional security inevitably involves making the system harder to use. Prelim. Resp. 41.

Patent Owner also asserts that Deibert's teaching that there is a "code relating to a timer that automatically deactivates *any mobile payment application*" is directed to payment applications, not authentication applications. Prelim. Resp. 42–43. In Deibert, Patent Owner suggests, deactivation is directed to the mobile payment applications—the payment application facilitates payment transaction and must be running for the transaction to be completed. *Id.* In fact, the mobile payment application in Deibert serves a different function than the authentication application in Brand—i.e., Deibert's mobile payment application simply completes a transaction, but Brand's authentication application performs the act of confirming or denying the transaction. In Brand, the authentication application must be running for the user to receive the pop-up which confirms the transaction (Pet. 36 (citing Ex. 1005, 7:6–15, 7:25–29), while in Deibert, the transaction is already authorized and the mobile payment application must be running only to send the contactless transaction to the terminal (*see* Ex. 1007, 3:57–59; *see also* Pet. 22 (discussing Deibert's deactivation function)).

We agree with Patent Owner that Brand and Deibert operate in different ways (i.e., one-factor vs. two-factor authentication) and Petitioner combines different functions (mobile payment vs. authentication), without explaining sufficiently why those functions would have been combined. We are also not persuaded by Petitioner's conclusory references to saving

battery life, making Brand's application easier to use, and increasing security—particularly when balanced against the fact that Deibert's deactivation conflicts with Brand's stated ability to hold a session open through multiple transactions.

Finally, Patent Owner argues that the combination would not be "combining prior art elements . . . according to known methods . . . to yield predictable results." Prelim. Resp. 43–44. We agree. We are also not persuaded by Petitioner's assertion that because both Brand and Deibert are implemented in programming code, it would be a simple combination. Pet. 24. This statement, by itself, does not provide any rationale for combining the cited teachings and certainly does not provide a sufficiently "articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." *KSR*, 550 U.S. at 418 (quoting *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)).

In summary, based on the information set forth in the Petition and the testimony of Dr. McDaniel, we are not persuaded that Petitioner has demonstrated sufficiently both the motivation to combine these references and the reasonable expectation of success as to its ground based on Brand, Williams, and Deibert.

b. Brand and Williams

Petitioner argues that a person of ordinary skill would have been motivated to combine Brand and Williams. Pet. 18–21. Petitioner contends Brand and Williams are both directed to payment transaction authorization and two-factor authentication. *Id.* at 19 (citing Ex. 1005, Abstract, 10:59–62; Ex. 1006, Abstract, 8–11; McDaniel Decl. ¶ 76).

Petitioner argues Brand's two-factor authentication using a mobile phone is "desirable." *Id.* Specifically, according to Petitioner, a person of

ordinary skill in the art "would have recognized such techniques are desirable, as they increase the authentication system's security and reduce fraud where a third-party, acting as a user, initiates a transaction." *Id.* (citing McDaniel Decl. ¶ 77).

Petitioner contends that Williams's system of sending an SMS message to confirm transactions improves security. *Id.* at 19–20. Petitioner states "Williams' predetermined period of time during which a transaction may be authorized improves the security of Williams' system and assists in preventing the authorization of fraudulent transactions. Without any such time limit, a requested transaction would remain pending until the user responds. This could lead to the user unintentionally or mistakenly approving a transaction that the user did not request (i.e., a fraudulent transaction)." *Id.* (internal citations omitted (citing McDaniels Decl. ¶ 70)).

As to the motivation to combine Brand and Williams, Petitioner argues it would have been obvious to a person of ordinary skill in the art to employ a time limit (i.e., similar to Williams's time limit) in Brand's system, such that a user would have a limited period of time to validate that the user possesses the mobile device. Pet. 20 (citing Ex. 1003 ¶ 79). According to Petitioner:

> This would contribute to the overall security of the authentication system. Including a predetermined time period is a way to validate that the user possessed the mobile device between the time the user initiated the transaction at his computer and the transaction was confirmed (or denied) at the authentication server. Ex-1003, ¶ 80; Ex-1005, 10:48-50. If the authentication server has not received a confirmation message after the predetermined time interval expired, the authentication server would determine that the transaction is fraudulent. Ex-1003, ¶ 80. When a user does not approve a transaction in a timely

> manner, there is an increased risk that the transaction is fraudulent. Ex-1003, ¶ 80.

Id. (citing McDaniel Decl. ¶ 79). Additionally, according to Petitioner, it was known in the art that security is enhanced "by limiting the time when authentication is possible." *Id.* (quoting Ex. 1014, 17:4–5 (a supporting prior art reference (McCorkle) that is not part of the ground).

Finally, Petitioner contends a person of ordinary skill in the art would have had a reasonable expectation of success in making the combination. *Id.* at 20–21. Petitioner asserts "such a combination would have simply been combining prior art elements (Williams' time-limited window for responding and Brand's accept/deny message) according to known methods (rejecting transactions for which a timely response is not received) to yield predictable results (validating that the user possesses the mobile device at the time of a transaction)." *Id.* at 20 (citing McDaniel Decl. ¶ 81). Petitioner further argues the combination of Brand and Williams is "merely the ordinary use of a common technique (limiting the time window for approving a transaction) to improve a similar two-factor authentication system in the same way (reducing fraudulent transactions)." *Id.* at 21. Petitioner supports these assertions with testimony from Dr. McDaniel. *See* McDaniel Decl. ¶¶ 75–81.

Patent Owner responds that Petitioner's argument for combining the references, as supported by Dr. McDaniel, are based on hindsight. Prelim. Resp. 53. Petitioner also asserts that "[w]hile Brand and Williams are generally related to payment transaction authorization, Brand explicitly discourages the use of Williams's SMS messaging application and teaches away from such an implementation." *Id.* at 50–51. Patent Owner cites Brand as "disparag[ing]" SMS messaging applications, calling them

"susceptible to abuse," "relatively high cost," and "prone to 'mistakes.'" *Id.* at 51. Patent Owner also asserts that the one embodiment in Brand that uses an SMS message is not related to timing and is not cited by Petitioner. *Id.* Thus, according to Patent Owner, a person of ordinary skill in the art "would not have combined Williams's SMS messaging system with Brand's system that forms its own direct, secure, and continuous connection between the mobile phone and the authentication server." *Id.* at 52.

Patent Owner asserts "a [person of ordinary skill in the art at the time of the invention], upon reading Brand and Williams, would . . . not have arrived at the claimed predetermined time relation." Prelim. Resp. 52. Patent Owner asserts that a person of ordinary skill in the art at the time of the invention would be led to an alternate solution, i.e., "would have implemented a system that counts down the time for Brand's user to select accept or deny on the pop-up notification on the user's mobile phone. That timer would have begun at the time that the pop-up notification appears on the user's mobile phone, not at a time that the user identification is transmitted over the first communication channel or a response is transmitted over a second communication channel." Prelim. Resp. 52–53.

We also agree with Patent Owner that the timer in Williams is used for a purpose, i.e., SMS messaging, that Brand disparages. Prelim. Resp. 51–52. We also agree with Patent Owner that Petitioner's arguments regarding motivation to combine the references are based on hindsight. Prelim. Resp. 53. For example, as explained further in Section III.B.2., *infra*, Petitioner does not explain why the predetermined time would start when the user enters their identification in a system when combining a direct message system with a system based on SMS messages and when neither reference has any disclosure about the start of the predetermined time. Thus,

we are not persuaded that Petitioner's articulated reasoning for why one of ordinary skill in the art would have been motivated to make the proposed combination is based on rational underpinnings. *See KSR Int'l Co.*, 550 U.S. at 418.

Petitioner's expert's declarant (McDaniel Decl. ¶¶ 75–81) essentially repeats the assertions of the Petition and provides no persuasive facts or data to support his opinion of obviousness. Therefore, we give such conclusory, unsupported assertions by Petitioner's expert little weight. *See In re Am. Acad. of Sci. Tech Ctr.*, 367 F.3d 1359, 1368 (Fed. Cir. 2004) ("[T]he Board is entitled to weigh the declarations and conclude that the lack of factual corroboration warrants discounting the opinions expressed in the declarations."); *see also* 37 C.F.R. § 42.65(a) ("Expert testimony that does not disclose the underlying facts or data on which the opinion is based is entitled to little or no weight.").

We are also not persuaded by Petitioner's assertion that the combination of Brand and Williams would have simply been combining prior art elements according to known methods to yield predictable results. This statement, by itself, does not provide any rationale for combining the cited teachings and certainly does not provide a sufficiently "articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." *KSR*, 550 U.S. at 418 (quoting *Kahn*, 441 F.3d 977 at 988). Petitioner does not explain persuasively how or why a person of ordinary skill would have combined the cited teachings. *See id.* ("Often, it will be necessary for a court to . . . determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue.").

In sum, we are not convinced that Petitioner has presented a sufficient rationale, apart from hindsight, demonstrating that a person of ordinary skill would have combined Brand with Deibert and/or Williams.

2. Teaching of Claim Limitations

In addition, even if Petitioner had sufficiently demonstrated that Brand, Williams, and Deibert would have been combined, the references in combination still would fail to teach or suggest at least one element of the challenged claims. Specifically, independent claim 1 recites, in relevant part, "as a criterion for deciding whether the authentication to the transaction shall be granted or denied, having the authentication device check whether a predetermined time relation exists between the transmission of the user identification and a response from the second communication channel" ("time window limitation"). Pet. 30–34. Petitioner has failed to persuade us that the references relied on in the Petition disclose this claimed feature.

Petitioner relies on the combination of Brand and Williams to meet this limitation. *Id.* Petitioner relies on Brand's teaching that authentication where a pop-up of the authentication application "requests the user (9) to either confirm (accept) or deny (reject) the transaction by means of an appropriate key press," and communicates a "result to [authentication] server" as the claimed deciding whether the authentication to the transaction shall be granted or denied. *Id.* at 30 (citing Ex. 1005, 7:6–13, 7:25–27). Petitioner also relies on Williams's authorization module, which checks if a "**return SMS message is received within a predetermined period of time**," as the claimed criterion. *Id.* (citing Ex. 1006, 11). As to the limitation "[a predetermined time relation exists] between the transmission of the user identification and a response," Petitioner relies on Williams teaching of "a user 'entering data concerning a transaction,' e.g. a card name and number

[*see* Ex. 1006, 9–10], and then transmitting a 'notification message to a predetermined mobile communication device.'" Pet. 32 (citing Ex. 1006, 6). Additionally, Petitioner states:

> It would have been obvious to a [person of ordinary skill in the art at the time of the invention] that this "predetermined period of time" would be measured from when the transaction was first initiated, i.e., starting at *the transmission of the user identification*. Ex-1003, p. 54.

Id. at 32–33. In other words, Petitioner relies on the knowledge of one of ordinary skill to show that the start of the predetermined time in Williams would be when the user information was sent. *Id.*[2]

Patent Owner asserts Williams's timer would not meet the limitation to starting the timer's predetermined time relation at "transmission of the user identification" because "William's [sic] timer begins counting down when the initial notification SMS message is sent to the phone, not when the user provides his user identification." Prelim. Resp. 48. Patent Owner acknowledges that Petitioner relies on the knowledge of one of ordinary skill in the art on page 32 of the Petition, but argues that "Petitioner and its expert have failed to show that the [person of ordinary skill in the art at the time of the invention] ***would have, not just could have,*** made the modification of the prior art to arrive at the claimed invention. Prelim. Resp. 49 (citing *Belden Inc. v. Berk-Tek LLC*, 805 F.3d 1064, 1073 (Fed. Cir. 2015)[3];

[2] The alleged motivation to combine these teachings is discussed in Section III.B.1.b., *supra*.
[3] Patent Owner cited "*Belden Inc. v. Berk-Tek LLC*, No. 14-1575 (Fed. Cir. 2015) 2015." Prelim. Resp. 49.

Metalcraft of Mayville, Inc. v. Toro Co., 848 F.3d 1358, 1367 (Fed. Cir. 2017)[4]).

Ultimately, Petitioner asserts:

> It would have been obvious to a [person of ordinary skill in the art at the time of the invention] to determine whether the time that Brand's user transmitted user information to the banking institution and the time the user transmitted a confirmation or denial result to the authentication server falls within the predetermined time period taught in Williams. Ex-1003, p. 55. This would make the authentication system more secure by adding a safeguard that validates that a person possessed the mobile device when the transaction was initiated and authenticated. It would also reduce fraudulent transactions because transactions would not authenticate if the time interval exceeds the predetermined time period. Ex-1003, p. 55. *See* Reasons to Combine Brand and Williams, § IX.C.4.

Id. at 33. In other words, Petitioner appears to state that, although neither Brand nor Williams teaches the time window of the claims, one of ordinary skill would have been motivated to modify Brand to add the claimed time window limitation to make the transaction more secure. We determine that this contention by Petitioner is speculative and based on hindsight. Petitioner's does not meet the standard set forth by the authorities requiring "specific reasoning, based on evidence of record, to support the legal conclusion of obviousness." *In re Magnum Oil Tools Int'l, Ltd.*, 829 F.3d 1364, 1380 (Fed. Cir. 2016). Thus, we are not persuaded by Petitioner's arguments.

Petitioner's expert essentially repeats the assertions of the Petition and provides no persuasive facts or data to support his opinion that the

[4] Patent Owner cites this case as "*Metalcraft of Mayville, Inc. v. The Toro Company*, No.-16-2433 (Fed. Cir. 2017)." Prelim. Resp. 49.

combination of Brand and Williams teaches these claim limitations. We give such conclusory, unsupported assertions by Petitioner's expert little weight. *See In re Am. Acad. of Sci. Tech Ctr.*, 367 F.3d at 1368 ("[T]he Board is entitled to weigh the declarations and conclude that the lack of factual corroboration warrants discounting the opinions expressed in the declarations."); *see also* 37 C.F.R. § 42.65(a) ("Expert testimony that does not disclose the underlying facts or data on which the opinion is based is entitled to little or no weight."); *Seabery N. Am., Inc. v. Lincoln Glob., Inc.*, IPR2016–00749, Paper 13 at 14 (PTAB Sept. 21, 2016) (Institution Decision). In the absence of persuasive argument or evidence, we determine Petitioner has failed to adequately show the combination of Brand and Williams teaches or suggests this limitation to a person of ordinary skill.

For at least the reasons discussed above, Petitioner has not demonstrated a reasonable likelihood of prevailing on its obviousness challenge based on Brand, Williams, and Deibert.

C. Challenge to Claims 5, 6, 7, 8, 10, and 11 based on Brand, Williams, Deibert, and Carter

Petitioner contends these claims would have been obvious over the combination of Brand, Williams, Deibert, and Carter. Pet. 44–67. Petitioner supports this assertion with testimony from Dr. McDaniel. McDaniel Decl. ¶¶ 94–115.

Patent Owner argues that Carter does not remedy the deficiencies of Brand, Williams, and Deibert as to teaching the limitations of claim 1. Prelim. Resp. 54. We agree. Petitioner does not rely on Carter as curing any of the deficiencies discussed above. Thus, based on the information set forth in the Petition and the testimony of Dr. McDaniel, we are not persuaded that Petitioner has demonstrated sufficiently both the motivation to combine

these references and the reasonable expectation of success as to its ground based on Brand, Williams, Deibert, and Carter.

D. Challenge to Claims 11 and 12 based on Brand, Williams, Deibert, Carter, and Nielsen

Petitioner contends these claims would have been obvious over the combination of Brand, Williams, Deibert, Carter, and Nielsen. Pet. 67–74. Petitioner supports this assertion with testimony from its expert, Dr. McDaniel. McDaniel Decl. ¶¶ 116–129.

Patent Owner argues that Nielsen does not remedy the deficiencies of Brand, Williams, and Deibert as to the limitation of claim 1. Prelim. Resp. 55–56. We agree. Petitioner does not rely on Nielsen as curing any of the deficiencies discussed above. Thus, based on the information set forth in the Petition and the testimony of Dr. McDaniel, we are not persuaded that Petitioner has demonstrated sufficiently both the motivation to combine these references and the reasonable expectation of success as to its ground based on Brand, Williams, Deibert, Carter, and Nielsen.

E. Challenge to Claim 13 based on Brand, Williams, Deibert, and Dietrich

Petitioner contends these claims would have been obvious over the combination of Brand, Williams, Deibert, and Dietrich. Pet. 74–80. Petitioner supports this assertion with testimony from its expert, Dr. McDaniel. McDaniel Decl., 130–142.

Patent Owner argues that Dietrich does not remedy the deficiencies of Brand, Williams, and Deibert as to the limitations of claim 1. Prelim. Resp. 56–57. We agree. Petitioner does not rely on Dietrich as curing any of the deficiencies discussed above. Thus, based on the information set forth in the Petition and the testimony of Dr. McDaniel, we are not persuaded that Petitioner has demonstrated sufficiently both the motivation to combine

these references and the reasonable expectation of success as to its ground based on Brand, Williams, Deibert, and Dietrich.

IV. CONCLUSION

We determine that Petitioner has not demonstrated a reasonable likelihood of prevailing on its challenges to claims 1–3, 5–8, and 10–13 of the '903 patent.

V. ORDER

Upon consideration of the record before us, it is:

ORDERED that the Petition is DENIED and no trial is instituted.

IPR2019-01638
Patent 9,246,903 B2

FOR PETITIONER:

David McCombs
Theodore Foster
Dina Blikshteyn
HAYNES AND BOONE, LLP
david.mccombs.ipr@haynesboone.com
ipr.theo.foster@haynesboone.com
dina.blikshteyn.ipr@haynesboone.com

FOR PATENT OWNER:

Scott Weingaertner
Grace Wang
WHITE & CASE LLP
scott.weingaertner@whitecase.com
grace.wang@whitecase.com

EXHIBIT C

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYSTEMS, INC.,
Petitioner,

v.

MONEY AND DATA PROTECTION LIZENZ GMBH & CO. KG
Patent Owner

IPR2019-01639
U.S. Patent No. 9,246,903

PETITION FOR *INTER PARTES* REVIEW UNDER 35 U.S.C. §312 AND 37 C.F.R. §42.104

Claims 14-17, 19, 21-22, and 24-26

TABLE OF CONTENTS

PETITIONER'S EXHIBIT LIST

September 24, 2019

Ex-1001	U.S. 9,246,903
Ex-1002	Prosecution History of U.S. 9,246,903
Ex-1003	Declaration of Patrick McDaniel, Ph.D., under 37 C.F.R. §1.68
Ex-1004	*Curriculum Vitae* of Patrick McDaniel, Ph.D.
Ex-1005	U.S. Patent No. 8,862,097 to Brand et al.
Ex-1006	U.K. Patent Application 2,398,159 to Williams
Ex-1007	U.S. Patent No. 9,647.855 to Deibert
Ex-1008	U.S. Publication No. 2011/0202466 to Carter
Ex-1009	*Reserved*
Ex-1010	*Reserved*
Ex-1011	U.S. Patent No. 8,306,532 to Rahman et al.
Ex-1012	U.S. Publication No. 2011/0050164 to Partovi at al.
Ex-1013	U.S. Patent No. 9,659,297 to Russell et al.
Ex-1014	U.S. Patent No. 7,039,392 to McCorkle et al.
Ex-1015	*Reserved*
Ex-1016	U.S. Patent No. 8,750,473 to Cook
Ex-1017	U.S. Patent No. 8,175,535 to Mu
Ex-1018	U.S. Patent No. 7,248,017 to Cheng et al.
Ex-1019	U.S. Patent No. 6,184,652 to Yang

Ex-1020	Patrick McDaniel. Computer and Network Authentication. *Handbook of Information Security*, John Wiley and Sons. September 2006. *Editor*: Hossein Bidgoli. URL: http://patrickmcdaniel.org/pubs/mcdaniel-netauth.pdf
Ex-1021	Patrick McDaniel. Authentication. *The Internet Encyclopedia*, John Wiley and Sons. 2002. URL: http://patrickmcdaniel.org/pubs/mcdaniel-authentication.pdf
Ex-1022	Anthony Nicholson, Mark D. Corner, and Brian D. Noble, "Mobile Device Security using Transient Authentication," *IEEE Transactions on Mobile Computing*, 5(11):1489–1502, November 2006.
Ex-1023	*Reserved*
Ex-1024	Information Disclosure Statement submitted in U.S. App. No. 12/334,957 on June 3, 2009.

I. INTRODUCTION

Pursuant to 35 U.S.C. §§ 311, 314(a), and 37 C.F.R. § 42.100, Cisco Systems, Inc. ("Petitioner") respectfully requests that the Board review and cancel as unpatentable under (pre-AIA) 35 U.S.C. §103(a) claims 14-17, 19, 21-22, and 24-26 (hereinafter, the "Challenged Claims") of U.S. 9,246,903 ("'903 Patent," Ex-1001).

The '903 Patent describes two-factor authentication technology for authenticating a user to a transaction. As shown below and in the Declaration of Patrick McDaniel (Ex-1003), these concepts were well-known before the '903 Patent was filed. The primary reference ("Brand," Ex-1005), describes a two-factor authentication system. The other claimed concepts—such as deactivating an application and a mobile device with a controller and a transceiver—were also well-known and obvious to combine. The combination of prior art concepts in the Challenged Claims was obvious.

II. MANDATORY NOTICES

A. Real Party-in-Interest

Pursuant to 37 C.F.R. § 42.8(b)(1), Petitioner certifies that the real parties-in-interest are Cisco Systems, Inc. and Duo Security, Inc.

B. Related Matters

Pursuant to 37 C.F.R. § 42.8(b)(2), to the best knowledge of the Petitioner,

the ’903 Patent is involved in the following cases:

Case Heading	Number	Court	Filed
Money and Data Protection Lizenz GmbH & Co. KG v. Duo Security, Inc.	1-18-cv-01477	DED	September 25, 2018

Petitioner is also concurrently filing a petition for *inter partes* review of claims 1-3, 5-8, and 10-13 of the ’903 Patent.

C. Lead and Back-up Counsel and Service Information

Lead Counsel
David L. McCombs
HAYNES AND BOONE, LLP
2323 Victory Ave. Suite 700
Dallas, TX 75219
Phone: (214) 651-5533
Fax: (214) 200-0853
david.mccombs.ipr@haynesboone.com
USPTO Reg. No. 32,271

Back-up Counsel
Theodore M. Foster
HAYNES AND BOONE, LLP
2323 Victory Ave. Suite 700
Dallas, TX 75219
Phone: (972) 739-8649
Fax: (214) 200-0853
ipr.theo.foster@haynesboone.com
USPTO Reg. No. 57,456

Dina Blikshteyn
HAYNES AND BOONE, LLP
2323 Victory Ave. Suite 700
Dallas, TX 75219
Phone: (212) 835-4809
Fax: (214) 200-0853
dina.blikshteyn.ipr@haynesboone.com
USPTO Reg. No. 63,962

Please address all correspondence to lead and back-up counsel. Petitioner consents to service in this proceeding by email at the addresses above.

III. GROUNDS FOR STANDING

Petitioner certifies that the ’903 Patent is eligible for *inter partes* review

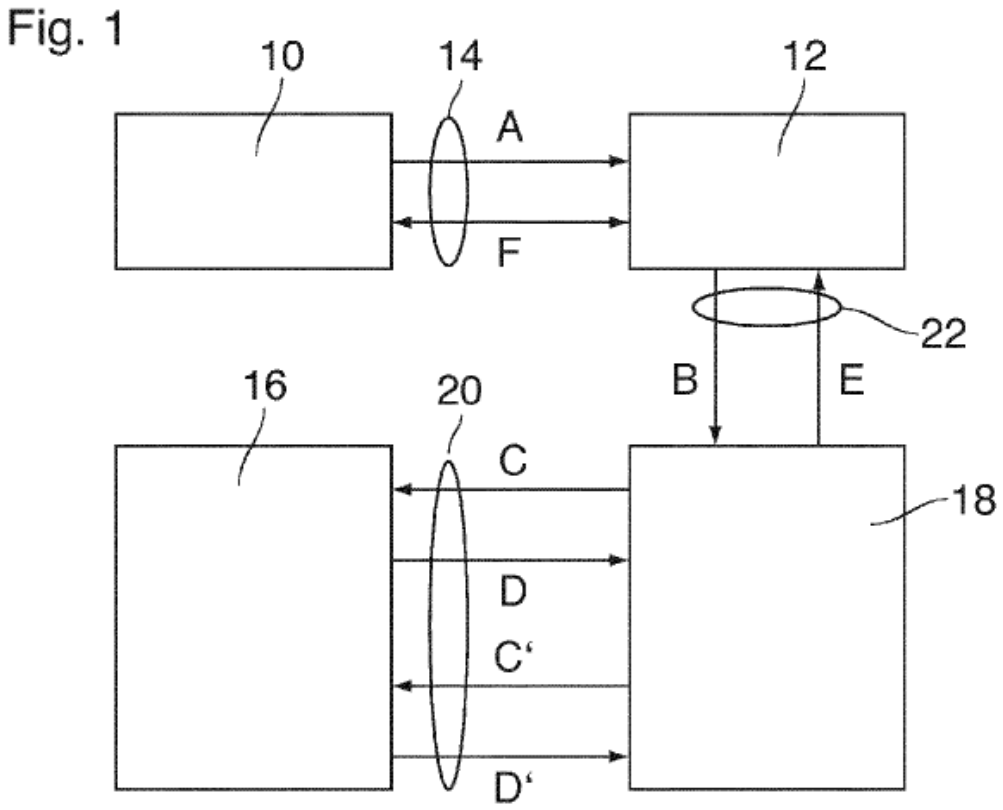
("IPR") and that Petitioner is not barred or estopped from challenging the patent claims on the grounds identified. 37 C.F.R. § 42.104(a).

IV. NOTE

Unless otherwise noted, all emphasis in any quoted material has been added.

V. '903 PATENT

The '903 Patent describes "authenticating a user to a transaction." Ex-1001, 1:3-4. The authentication system, illustrated in Fig. 1 below, includes transaction terminal 10, remote transaction partner 12, mobile communication device 16, and authentication device 18. Ex-1001, 4:41-45. Up to three separate communication channels (14, 20, 22) link the components. Ex-1001, 4:39-49.



Ex-1001, FIG. 1

VI. LEVEL OF ORDINARY SKILL

A Person of Ordinary Skill in The Art ("POSITA") in October 2011 would have had a working knowledge of the authentication art that is pertinent to the '903 Patent, including two-factor authentication using a mobile device. A POSITA would have had a bachelor's degree in computer science, computer engineering, or an equivalent, and three years of professional experience. Lack of professional experience can be remedied by additional education, and vice versa. Ex-1003, ¶¶ 15-19.

VII. CLAIM CONSTRUCTION

This Petition analyzes claims according to their ordinary and customary meaning as would be understood by one of ordinary skill in the art in view of the specification. *Phillips v. AWH Corp*., 415 F.3d 1303 (Fed. Cir. 2005) (*en banc*); Ex-1003, ¶¶ 49-50.

Various claims recite quasi-Markush terms (*see* M.P.E.P. 2117), which are construed below.

A. "deactivate the authentication function one of: after it has been active for a predetermined time interval after its state has been checked."

This limitation, recited in claim 14, was expressly amended to remove the words "and" and "or" between two potential Markush group alternatives. *See* Ex-1002, 56. Thus, the plain language recites a single limitation, not alternatives. Accordingly, a plain and ordinary meaning of this claim language is: *deactivate the authentication function after it has been active for a predetermined time interval after its state has been checked*. Ex-1003, ¶ 56.

Alternatively, the specification describes multiple embodiments for timing the deactivation of the authentication function. This petition shows that the limitation is taught even if interpreted as a Markush group, i.e.: *deactivate the authentication function (1) after it has been active for a predetermined time interval* or *(2) after its state has been checked*. Ex-1003, ¶ 57.

B. "wherein the connector is one of a USB connector and a micro-USB connector."

This limitation is recited in claim 17. The '903 Patent describes a "USB socket" and a "micro-USB socket" as alternatives. Ex-1001, 8:59-62. Accordingly, a plain and ordinary meaning of this limitation is *wherein the connector is (1) a USB connector* or *(2) a micro-USB connector*. Ex-1003, ¶ 58.

C. "an acoustic transducer for providing an acoustic feedback signal upon at least one of activation and deactivation of the authentication function."

This limitation is recited in claim 26. The '903 Patent describes "a buzzer 49 is provided for giving an acoustic feedback when the authentication function has been activated." Ex-1001, 8:50-52. Accordingly, for the purposes of this proceeding, a plain and ordinary meaning of this limitation is: *an acoustic transducer for providing an acoustic feedback signal upon (1) activation of the authentication function* or *(2) deactivation of the authentication function*. Ex-1003, ¶ 59.

VIII. RELIEF REQUESTED AND REASONS THEREFORE

Petitioner asks that the Board institute a trial for *inter partes* review of the Challenged Claims and cancel these claims.

IX. IDENTIFICATION OF HOW THE CLAIMS ARE UNPATENTABLE

A. Challenged Claims

This Petition challenges claims 14-17, 19, 21-22, and 24-26 of the '903

Patent.

B. Statutory Grounds for Challenges

Ground	Claim(s)	Basis
n/a[1]	1	35 U.S.C. § 103 (Pre-AIA) over Brand, Williams, and Deibert
#1	14, 21, 24, 25, and 26	35 U.S.C. § 103 (Pre-AIA) over Brand, Williams, Deibert, and Rahman
#2	15, 16, and 17	35 U.S.C. § 103 (Pre-AIA) over Brand, Williams, Deibert, Rahman, and Partovi
#3	19	35 U.S.C. § 103 (Pre-AIA) over Brand, Williams, Deibert, Rahman, and Carter
#4	22	35 U.S.C. § 103 (Pre-AIA) over Brand, Williams, Deibert, Rahman, and Russell

U.S. Patent No. 8,862,097 to Brand (Ex-1005, "Brand") was filed on December 3, 2009.

U.K. Patent Application GB2,398,159 to Williams (Ex-1006, "Williams") published on August 11, 2004. Williams' publication status is confirmed by its citation on an Information Disclosure Statement by the applicants in U.S. App. No. 12/334,957 on June 3, 2009. *See* Ex-1024.

U.S. Patent No. 9,647,855 to Deibert (Ex-1007, "Deibert"), was filed on

[1] All challenged claims depend from claim 1, thus requiring this petition to address its limitations.

January 9, 2008.

U.S. Publication No. 2011/0202466 to Carter (Ex-1008, "Carter"), was filed on October 19, 2009.

U.S. Patent No. 8,306,532 to Rahman (Ex-1011, "Rahman") was filed on June 26, 2009.

U.S. Publication No. 2011/0050164 to Partovi (Ex-1012, "Partovi") was filed on April 28, 2010.

U.S. Patent No. 9,659,297 to Russell (Ex-1013, "Russell") was filed on August 7, 2008.

Brand, Deibert, Carter, Rahman, Partovi, and Russell are prior art under 35 U.S.C. § 102(e).

Williams is prior art under 35 U.S.C. § 102(b).

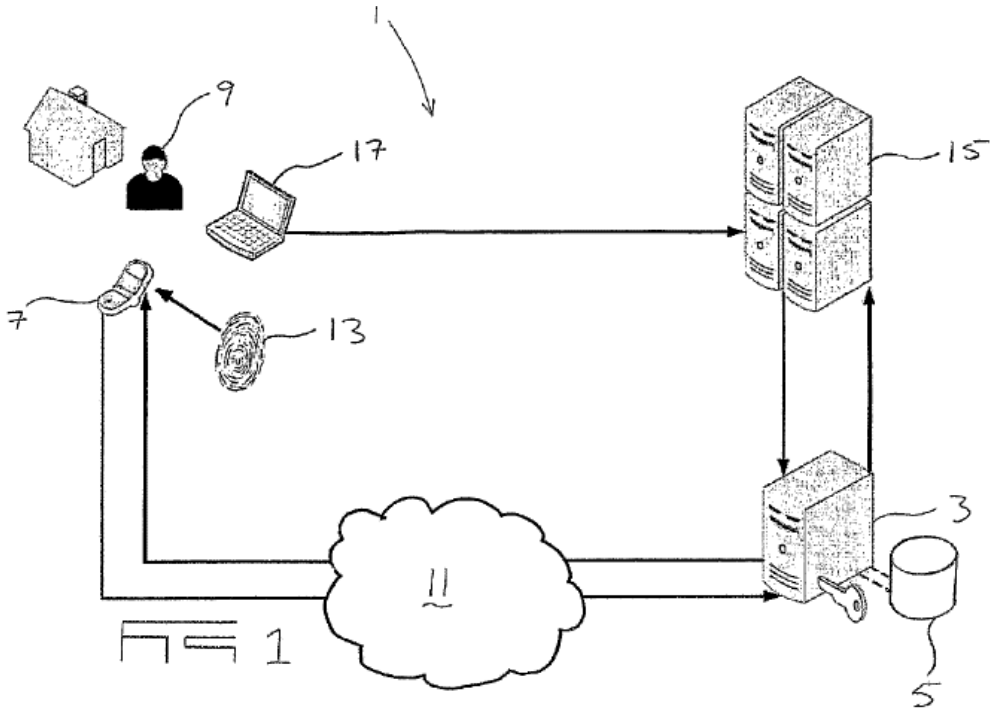
Petitioner's proposed combinations permit but do not require the physical incorporation of elements. *See In re Mouttet*, 686 F.3d 1322, 1332 (Fed. Cir. 2012); Ex-1003, ¶ 64.

C. Preliminary: Claim 1 is obvious over Brand, Williams, and Deibert

1. Brand

Like the '903 Patent, Brand (Ex-1005) discloses a system "for authenticating secure transactions between a transacting user and a secure transaction host." Ex-

1005, Abstract. Figure 1 (below) shows Brand's authentication system including a user (9), user's computer (17), banking institution (15), user's mobile phone (7), and authentication server (3). Ex-1005, 5:44, 6:48-55.



Ex-1005, FIG. 1

Brand discloses that "to log into his or her internet banking account, the user (9) first accesses the website of the banking institution (15) at which his or her account is held, from a personal computer (17), laptop or other Internet enabled device." Ex-1005, 6:47-50. The user "enters his account number (equivalent to a username) and password on the Internet banking website on his computer." Ex-1005, 6:50-53.

"Before proceeding to login, the user (9) initiates the authentication application on his/her mobile phone." Ex-1005, 6:53-55. The authentication application establishes a "real-time communication link" via "a GSM network" between "the authentication server" and "the mobile phone." Ex-1005, 6:62-64, 5:67.

"Upon the user (9) requesting login to his internet banking account, the banking institution (15) requests authentication of the user (9) from the authentication server." Ex-1005, 7:1-3. The authentication server "sends a transaction confirmation request to the mobile phone (7) which is received by the software application." Ex-1005, 7:3-6. The "software application triggers a pop-up on the monitor of the mobile phone" which allows "the user (9) to either confirm (accept) or deny (reject) the transaction." Ex-1005, 7:6-12.

If the user "confirms the transaction, the application communicates this confirmation result to the server" which "sends a positive authentication result to the banking institution server." Ex-1005, 7:12-15. The banking institution then allows the user "to proceed to its Internet banking account." Ex-1006, 7:15-17.

2. Williams

Like Brand, Williams relates to "a transaction authorisation[2] system for electronic payments." Ex-1006, 8. Williams teaches that terminals are "linked to a card issuer's central transaction processing unit." Ex-1006, 8. The transaction processing unit has an authorisation module which causes a message generation module to transmit "a SMS message identifying the card account, the transaction data and time, the merchant and the transaction value..." to "a mobile communication device... for the card account." Ex-1006, 9. The account holder "sends a return SMS message... using his mobile device." Ex-1006, 10. If the "return SMS message is received within a predetermined period of time, the authorisation module 3 instructs the transaction processing unit to authorise the transaction." Ex-1006, 11.

3. Deibert

Deibert relates to mobile device payments. Ex-1007, Abstract. Deibert describes "mobile payment applications." Ex-1007, 6:45-48. An application includes "a timer that automatically deactivates any mobile payment application[] after a predetermined timeout time has elapsed." Ex-1007, 6:50-52.

[2] As a U.K. patent, Williams uses British English spellings.

4. Reasons to Combine Brand and Williams

A POSITA would have found it obvious to combine the teachings of Brand and Williams for multiple reasons, including to obtain predictable and beneficial results that validate that the user possesses the mobile device while conducting a transaction. Ex-1003, ¶ 75.

First, a POSITA, when considering the teachings of Brand, would have also considered the teachings of Williams since they are analogous prior art pertaining specifically to payment transaction authorization and two-factor authentication. Ex-1005, Abstract, 10:59-62; Ex-1006, Abstract, 8-11; Ex-1003, ¶ 76.

Second, the two authentication factors in Brand are "something the person to be authenticated has" (e.g., a mobile device) and "something he or she knows (for example a username and password)." Ex-1005, 2:40-44. Requiring "the user to interactively confirm (accept) or deny (reject) the transaction" validates that the user possesses the mobile device. Ex-1005, 10:46-48. A POSITA would have recognized such techniques are desirable, as they increase the authentication system's security and reduce fraud where a third-party, acting as a user, initiates a transaction. Ex-1003, ¶ 77.

Williams similarly describes authenticating a transaction via a user's mobile phone. Ex-1006, Abstract. When a transaction is requested, Williams' system sends an SMS message to the user's mobile phone. Ex-1006, 10. The transaction is

authorized only if the user's "return SMS message" is "received within a predetermined period of time." Ex-1006, 11.

A POSITA would have recognized that Williams' predetermined period of time during which a transaction may be authorized improves the security of Williams' system and assists in preventing the authorization of fraudulent transactions. Ex-1003, ¶ 79. Without any such time limit, a requested transaction would remain pending until the user responds. This could lead to the user unintentionally or mistakenly approving a transaction that the user did not request (i.e., a fraudulent transaction). Ex-1003, ¶ 79.

It would have been obvious to a POSITA to employ a similar time limit in Brand's system, such that a user would have a limited period of time to validate that the user possesses the mobile device. Ex-1003, ¶ 79. This would contribute to the overall security of the authentication system. Including a predetermined time period is a way to validate that the user possessed the mobile device between the time the user initiated the transaction at his computer and the transaction was confirmed (or denied) at the authentication server. Ex-1003, ¶ 80; Ex-1005, 10:48-50. If the authentication server has not received a confirmation message after the predetermined time interval expired, the authentication server would determine that the transaction is fraudulent. Ex-1003, ¶ 80. When a user does not approve a transaction in a timely manner, there is an increased risk that the transaction is

fraudulent. Ex-1003, ¶ 80. More generally, it was known in the art that security is enhanced "by limiting the time when authentication is possible." Ex-1014, 17:4-5.

Third, such a combination would have simply been combining prior art elements (Williams' time-limited window for responding and Brand's accept/deny message) according to known methods (rejecting transactions for which a timely response is not received) to yield predictable results (validating that the user possesses the mobile device at the time of a transaction). Ex-1003, ¶ 81. Additionally, the combination of Brand and Williams is merely the ordinary use of a common technique (limiting the time window for approving a transaction) to improve a similar two-factor authentication system in the same way (reducing fraudulent transactions). Ex-1003, ¶ 81.

5. Reasons to Combine Brand and Deibert

A POSITA would have found it obvious to combine the teachings of Brand and Deibert for multiple reasons, including to produce the obvious, beneficial, and predictable result of automatically deactivating the authentication application. Ex-1003, ¶ 83.

First, a POSITA, when considering the teachings of Brand, would have also considered the teachings of Deibert since they are analogous prior art pertaining to payment systems. Ex-1005, Abstract; Ex-1007, Abstract. Both Brand and Deibert

describe authentication features that prevent fraud. Ex-1005, Abstract; Ex-1007, 9:27-30; Ex-1003, ¶ 84.

Second, Brand teaches that a user "initiates the authentication application on his/her mobile phone." Ex-1005, 6:53-54. A POSITA would have recognized that once initiated, the authentication application would execute on mobile device until the application is deactivated or the mobile device loses power. Ex-1003, ¶ 85. During that time, the authentication application would consume resources including battery power. Accordingly, a POSITA would have recognized that automatically deactivating the authentication application would have been desirable. Ex-1003, ¶ 85.

Deibert teaches software "code relating to a timer that automatically deactivates any mobile payment applications." Ex-1007, 6:49-53. A POSITA would have been motivated to combine Deibert's teachings that describe the deactivation code with Brand's authentication application so that the authentication application would deactivate automatically. Ex-1003, ¶ 86. In this way, the authentication application does not needlessly execute on the mobile device and consume system resources, *e.g.*, the processor, memory, and battery (which can be used to process other applications). Ex-1003, ¶ 87. Automatically deactivating the authentication application would also make the application easier to use because the user would not have to remember to manually deactivate the application after

accepting (or denying) the transaction. Ex-1003, ¶ 88. Additionally, if a user has a predetermined period of time during which a user can authenticate a transaction, it would have been obvious to a POSITA for the authentication application to automatically deactivate after the amount of the predetermined period of time expired, since any response would be untimely and therefore moot. Ex-1003, ¶ 88.

Third, Deibert describes "code relating to a timer that automatically deactivates... applications after a predetermined timeout time has elapsed." Ex-1007, 6:49-53. A POSITA would have been motivated to include a timer that begins to count down for a predetermined time before deactivating Brand's authentication application. Ex-1003, ¶ 89. This would beneficially save resources of the mobile device. Ex-1003, ¶ 89. This would also increase security of the authentication system, because once deactivated, the authentication application would require the user to reinitiate the application using user's credentials and prevent a third-party from using the authentication application. Ex-1005, 6:53-55, 8:51-56; Ex-1003, ¶ 89. Confirming this, Brand teaches that "a person who comes into possession of the mobile phone illegally will not even be able to activate the software application, let alone establish the communications link with the authentication server." Ex-1005, 8:53-56.

A POSITA looking to implement the deactivation code would recognize that the predetermined time period would need to start upon the occurrence of some

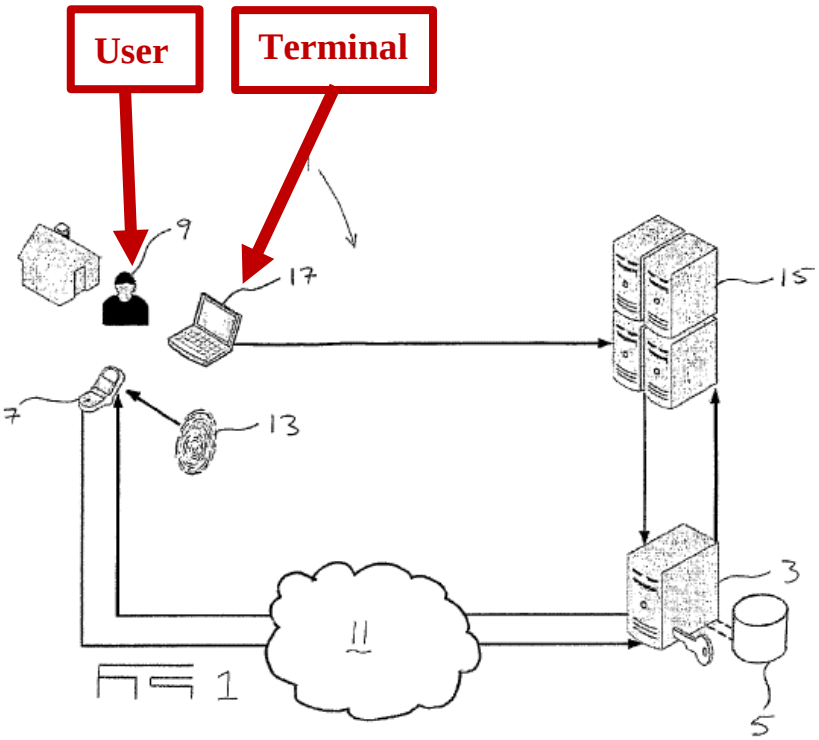
event. Ex-1003, ¶ 90. An obvious event to start a timer would be when the authentication application is initiated. Ex-1003, ¶ 90; Ex-1005, 6:53-55. In this case, the timer would be long enough for the user to authenticate a transaction. Another obvious event would be when the authentication server received a message confirming/denying the transaction, since at that point the authentication application has fulfilled its purpose. Ex-1003, ¶ 90; Ex-1005, 6:53-55; 7:12-13, 7:25-29. Either of those events would allow the user to authenticate the transaction while safeguarding the security of the authentication system and preserving resources of the mobile device. Ex-1003, ¶ 90.

Fourth, a POSITA would have been familiar with conventional coding languages, such as Java, C++ or Perl, used to write software applications. Ex-1003, ¶ 91; *see also* Ex-1007, 10:47-50; Ex-1005, 9:25-26, 9:40-46; Ex-1001, 4:52-53, 6:22-38. A POSITA would have considered this information when using Deibert's code that "automatically deactivates" an application after a predetermined time period has lapsed with Brand's authentication application. Ex-1003, ¶ 91. The combination is simply combining prior art elements (Deibert's timer that automatically deactivates Brand's authentication application) according to known methods (code written in a programming language) to yield predictable results (automatically deactivating the authentication application). Ex-1003, ¶ 91.

6. Claim 1

[1.0] ***A method of authenticating a user to a transaction at a terminal, comprising the steps of:***

Brand discloses the preamble. Brand discloses "[a] ***method*... for *authenticating* secure *transactions* between a transacting *user*** and a secure transaction host." Ex-1005, Abstract. Brand further discloses that the user performs a log-in process (a *transaction*) from a *terminal* such as "**a personal computer (17), laptop or other Internet enabled device**." Ex-1005, 6:47-50; Ex-1003, p. 43. Brand's system is shown in Figure 1:



Ex-1005, FIG. 1 (Annotated); Ex-1003, p. 44

Accordingly, Brand discloses a method of authenticating a user to a transaction conducted on a computer, which discloses "*[a] method of authenticating a user to a transaction at a terminal*." Ex-1003, p. 44.

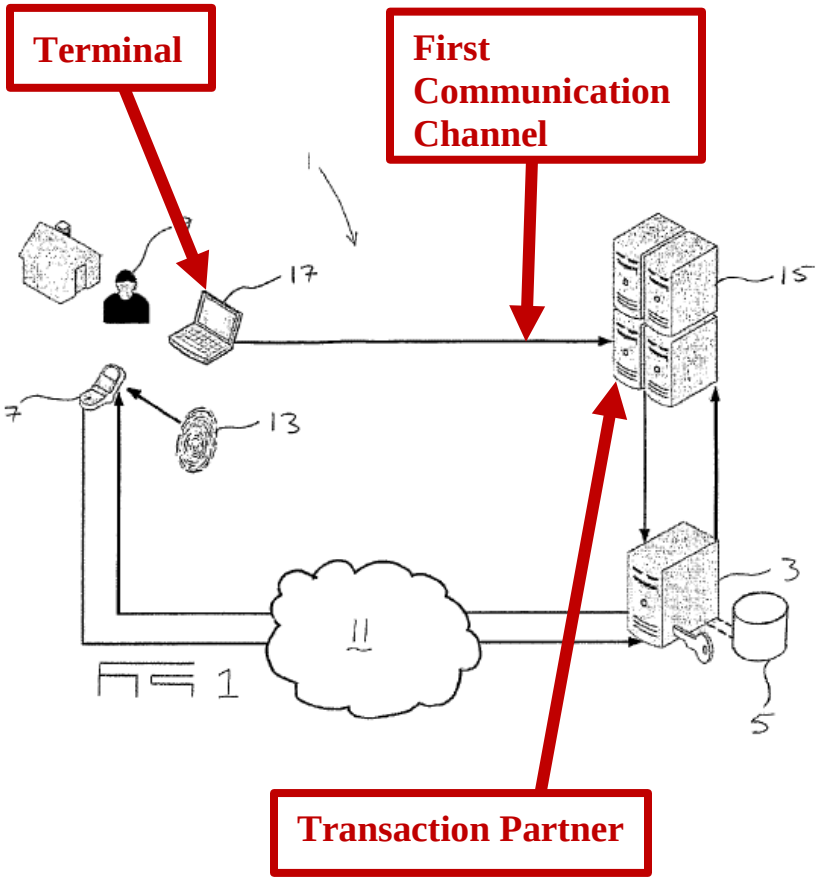
[1.1] ***transmitting a user identification from the terminal to a transaction partner via a first communication channel;***

Brand discloses this limitation. First, Brand discloses the user "requesting login to his internet banking account" at a banking institution. Ex-1005, 7:1-3. The user logs in by "enter[ing] his **account number (equivalent to a username) and password** on the Internet banking website **on his computer**." Ex-1005, 6:51-53. The user's account number is a *user identification* because it identifies the user to a banking institution, and the banking institution operating the Internet banking website is a *transaction partner*. Ex-1003, pp. 44-45; Ex-1006, 1:47-53. As discussed in [1.0], the user's computer is the *terminal*. Ex-1003, p. 46.

Brand discloses that the account number is *transmit[ted]* to the banking institution because "the banking institution (15) requests authentication of the user" upon user logging in by entering "his account number... and password." Ex-1005, 7:1-3, *see also id*. 66:50-53, Fig. 1 (line from 17 to 15); Ex-1003, p. 45. It would have been obvious that the account number and password are transmitted to the banking institution. Ex-1003, p. 45.

Second, Brand discloses that the user "first accesses **the website of the banking institution**... from a personal computer (17), laptop or other **Internet enabled device**." Ex-1005, 6:48-50. The Internet connection between the user's computer and the banking institution is a *first communication channel*. Ex-1003, ¶ p. 45.

Brand's Figure 1 illustrates the computer (*terminal*), the banking institution (*transaction partner*), and an Internet enabled connection between the computer and the banking institution (*first communication channel*). Ex-1005, Figure 1.



Ex-1005, FIG. 1 (Annotated); Ex-1003, p. 46

Accordingly, Brand discloses transmitting an account number (username) over an Internet connection from the user's computer to the banking institution, which discloses "*transmitting a user identification from the terminal to a transaction partner via a first communication channel*." Ex-1003, p. 46.

[1.2] *providing an authentication step in which an authentication device uses a second communication channel for checking an authentication function that is implemented in a mobile device of the user,*

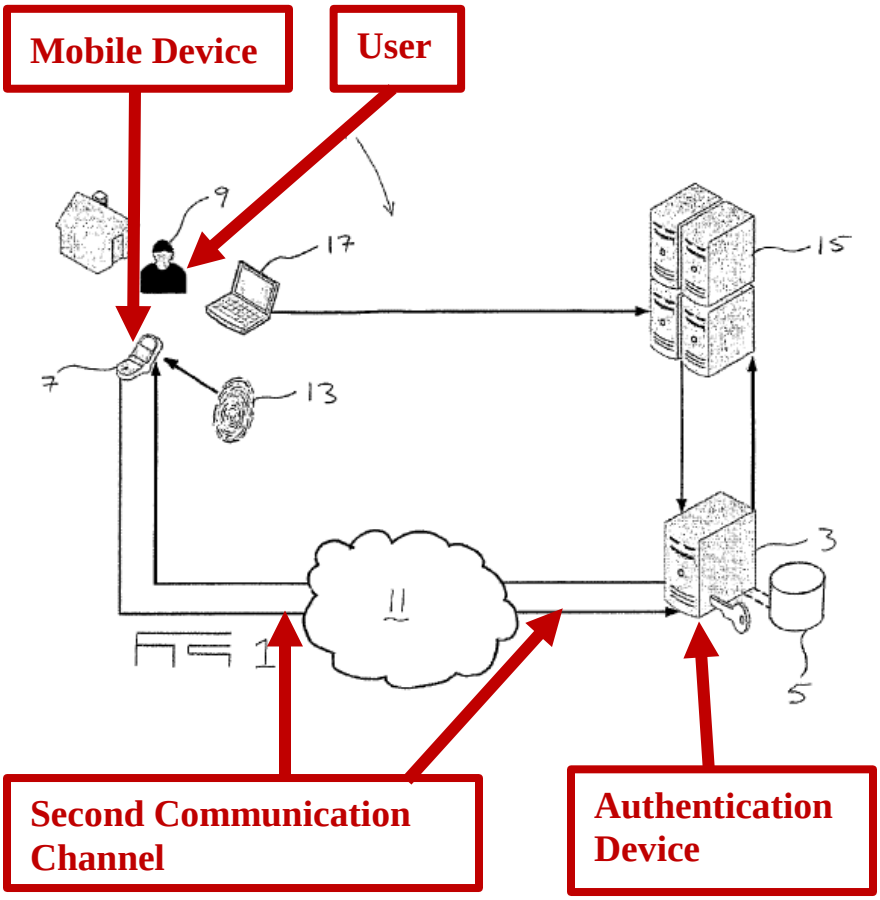
Brand discloses this limitation. First, Brand discloses *an authentication step* where "the banking institution (15) requests authentication of the user (9) from the authentication server." Ex-1005, 7:1-3. The authentication server is an *authentication device*. Ex-1003, pp. 46-47.

During the *authentication step*, "the **authentication server (3)** in turn **sends a transaction confirmation request to the mobile phone (7) which is received by the software application**." Brand, 7:3-6. Brand discloses that "the user (9) initiates the **authentication application**" (*authentication function*) "**on his/her mobile phone**," which is "a *mobile* communication *device*." Ex-1005, 6:53-54; 5:46-48; Ex-1003, p. 47. Thus, the authentication application on the mobile phone discloses *an authentication function that is implemented in a mobile device of the user*. Ex-1003, pp. 47-48.

Second, Brand discloses that a "**[c]ommunication between the application on the mobile phone (7) and the authentication server (3) takes place via a**

GSM network" which provides a "real-time communication link." Ex-1005, 5:65-6:3, 6:53-54. The GSM network communication link is a *second communication channel*. Ex-1003, p. 48.

Brand's Figure 1 (below) illustrates an authentication server (*authentication device*), a mobile phone (*mobile device*) of a user, and a GSM network communication link (*second communication channel*):



Ex-1005, FIG. 1 (Annotated); Ex-1003, p. 49

Accordingly, Brand discloses an authentication server that authenticates a user by sending a request over a GSM network communication link to an

authentication application in a user's mobile device, which discloses "*providing an authentication step in which an authentication device uses a second communication channel for checking an authentication function that is implemented in a mobile device of the user*." Ex-1003, p. 49.

[1.3.1] ***as a criterion for deciding whether the authentication to the transaction shall be granted or denied, having the authentication device check whether a predetermined time relation exists ...***

Brand and Williams render this limitation obvious. First, Brand discloses authentication where a pop-up of the authentication application "requests the user (9) to either confirm (accept) or deny (reject) the transaction by means of an appropriate key press," and communicates a "result to [authentication] server." Ex-1005, 7:6-13, 7:25-27. The authentication server (*authentication device*) checks the result because the server sends a corresponding positive or negative "authentication result" to a banking institution. Ex-1005, 7:13-15, 7:25-29; 8:25-32. Ex-1003, pp. 49-50.

Second, Williams, which like Brand authenticates the user, teaches an authorisation module that causes an SMS message "identifying the card account, the transaction data and time, the merchant and the transaction value" to be sent "to the account holder's nominated mobile device." Ex-1006, 9-10. The authorisation module *check[s]* if a "**return SMS message is received within a predetermined period of time**," which is a *criterion*. Ex-1006, 11. If so, *the transaction shall be*

granted because "the authorisation module 3 instructs the transaction processing unit 2 to **authorise the transaction**." Ex-1006, 11. "[I]f no such SMS message is received within this time, **the transaction is not authorised**," and *the transaction shall be denied*. Ex-1006, 11. The predetermined period of time taught in Williams is *a predetermined time relation* which is checked "*for deciding whether the authentication to the transaction shall be granted or denied*." Ex-1003, p. 51.

It would have been obvious to a POSITA for Brand's authentication server to check if a user's response is received within a predetermined time period, as taught by Williams. Ex-1003, p. 52. First, it would make the transaction more secure by validating that the user possessed the mobile device when he initiated the transaction at the terminal. Ex-1003, p. 52. Second, it would reduce fraudulent transactions because the authentication server would not authenticate transactions after the predetermined time period expired. Ex-1003, p. 52. *See* Reasons to Combine Brand and Williams, § IX.C.4.

Accordingly, Brand and Williams teach an authentication server that checks whether an authorization response was received during a predetermined time period, which renders obvious "*as a criterion for deciding whether the authentication to the transaction shall be granted or denied, having the authentication device check whether a predetermined time relation exists*." Ex-1003, p. 52.

[1.3.2] [a predetermined time relation exists] between the transmission of the user identification and a response from the second communication channel,

Brand and Williams render this limitation obvious. First, as discussed in [1.1], Brand discloses that the *terminal* transmits *user identification*. Ex-1003, p. 52.

Second, Brand discloses an authentication application communicating a confirmation or denial "result" (*response*) to the authentication server (*authentication device*). Ex-1005, 7:12-13, 7:25-29; Ex-1003, pp. 52-53.

Third, Williams teaches a user "entering data concerning a transaction," e.g. a card name and number, and then transmitting a "notification message to a predetermined mobile communication device." Ex-1006, 6. The user "reads the SMS message on his screen 7, and if it corresponds to a transaction of which he is aware, he sends a return SMS message." Ex-1006, 10. The authorisation module checks if "an appropriate return SMS message is received within a predetermined period of time." Ex-1006, 11. It would have been obvious to a POSITA that this "predetermined period of time" would be measured from when the transaction was first initiated, i.e., starting at the *transmission of the user identification*. Ex-1003, p. 54. For example, if the *relation* between the time that the user enters data (e.g. card name and number) and the time the user sends a return SMS message that confirms the transaction is within the predetermined time period (*predetermined time*), the

transaction is authorised. Ex-1003, p. 54. Alternatively, if a *relation* between the time the user enters data and the time the user sends a return SMS message is greater than the predetermined time period, the transaction is denied. Ex-1003, p. 54; Ex-1006, 11.

Fourth, as discussed in [1.2], Brand discloses that the mobile device and the authentication server communicate via a GSM network communication link (*second communication channel*). Thus, *the response* transmitted from the mobile device's authentication application to the authentication server is transmitted over the *second communication channel*. Ex-1003, pp. 54-55.

It would have been obvious to a POSITA to determine whether the time that Brand's user transmitted user information to the banking institution and the time the user transmitted a confirmation or denial result to the authentication server falls within the predetermined time period taught in Williams. Ex-1003, p. 55. This would make the authentication system more secure by adding a safeguard that validates that a person possessed the mobile device when the transaction was initiated and authenticated. It would also reduce fraudulent transactions because transactions would not authenticate if the time interval exceeds the predetermined time period. Ex-1003, p. 55. See Reasons to Combine Brand and Williams, § IX.C.4.

Accordingly, Brand and Williams teach permitting a transaction to be approved only during a limited time following the transaction's initiation, which renders obvious "*a predetermined time relation exists between the transmission of the user identification and a response from the second communication channel*." Ex-1003, p. 55.

[1.4] ***ensuring that the authentication function is normally inactive and is activated by the user only preliminarily for the transaction,***

Brand and Deibert render this limitation obvious. First, as discussed in [1.1], Brand discloses a *transaction* that a user initiated at a *terminal*, and as discussed in [1.2], Brand discloses an authentication application (*authentication function*). Ex-1003, p. 55.

Second, Brand discloses "[b]efore proceeding to login, the user (9) **initiates the authentication application** on his/her mobile phone." Ex-1005, 6:53-55. A POSITA would have understood that an authentication application was previously inactive because the user must initiate (*activate*) it. Ex-1003, pp. 55-56.

Third, in Brand the user initiates the authentication application "before proceeding to login" to the banking institution where the user conducts the transaction. Ex-1005, 6:53-54. Thus, Brand discloses "*ensuring that the authentication function... is activated by the user only preliminarily for the transaction*." Ex-1003, p. 56.

Fourth, Deibert teaches "a timer that **automatically deactivates** any mobile payment applications after a predetermined timeout time has elapsed." Ex-1007, 6:49-53. The "timer... begins counting down" when "the mobile phone is ready to conduct a transaction." Ex-1007, 9:35-38. A POSITA would have recognized that setting a timer that begins a countdown from a predetermined time period after an application is ready to conduct a transaction *ensure[s]* that the application is deactivated and "*is normally inactive*." Ex-1003, pp. 56-57

In light of Deibert's teachings, it would have been obvious to a POSITA for Brand's authentication application to include a timer that automatically deactivates the authentication application. Ex-1003, p. 57. This would make the authentication system more secure because a third-party who steals the user's mobile device would not be able to fraudulently authenticate a transaction without first initiating the authentication application. Ex-1003, p. 57. This also conserves mobile device resources. Ex-1003, p. 57. *See* Reasons to Combine Brand and Deibert, § IX.C.5.

Accordingly, Brand in combination with Deibert teaches that the authentication application is activated prior to proceeding with a login to conduct a transaction and is deactivated after a predetermined time period, which renders obvious "*ensuring that the authentication function is normally inactive and is activated by the user only preliminarily for the transaction*." Ex-1003, p. 57.

[1.5] ***ensuring that said response from the second communication channel includes information that the authentication function is active,***

Brand discloses this limitation. First, as discussed in [1.3.1], Brand discloses a result (*response*) transmitted from the authentication application (*authentication function*) to the authentication server via the GSM network communication link (*second communication channel*). Ex-1005, 7:12-15, 7:25-29; Ex-1003, p. 57. The authentication "application triggers a pop-up" through which the user confirms or denies the transaction, and then generates a "confirmation" or "denial" result. Ex-1005, 7:6-15, 7:25-29. Brand further explains that the pop-up to obtain a user's approval is optional. Ex-1005, 10:45-48 ("…a secure transaction ***may*** require the user to interactively confirm…"). It would have been obvious to a POSITA for the authentication application to be configurable to either present or suppress the individual transaction confirmation requests because Brand discloses that the pop-up behavior can be "configured." Ex-1005, 14:30-37; Ex-1003, pp. 58-59. Where the user has configured the authentication application to suppress the confirmation requests, the authentication application would immediately respond to the message received from the authentication server. Thus, the authentication application "provides a way of using a person's mobile phone to uniquely identify the user for authentication purposes" simply because the authentication application was active. Cf. Ex-1005, 10:48-50. Any of these potential response messages from the

authentication application to the authentication server would have demonstrated to the authentication server that the authentication application is *active*. Thus it would have been obvious to a POSITA for Brand's response message to *include[] information that the authentication function is active*. Ex-1003, pp. 58-59.

Second, Brand discloses that the authentication server checks that the authentication application is *active* because the authentication server receives and reads the result message from the authentication application to determine "if the authentication was successful." Ex-1005, 7:8-15, 7:25-29, 8:25-32; Ex-1003, p. 59. Based on the type of the result, the authentication server sends a "positive" or "negative" authentication result to the banking institution server. Ex-1005, 7:8-15, 7:27-29.

Accordingly, Brand discloses that the authentication application is used to generate a result and transmits the result to the authentication server which checks the result, which discloses "*ensuring that said response from the second communication channel includes information that the authentication function is active*," as claimed. Ex-1003, p. 59.

[1.6] ***thereafter ensuring that the authentication function is automatically deactivated.***

Brand and Deibert render this limitation obvious. First, as discussed in [1.2], Brand discloses an authentication application (*authentication function*) that executes on a mobile device, and as discussed in [1.5], the authentication application generates a result (*information that the authentication function is active*). Ex-1003, p. 59.

Second, as discussed in [1.4], Deibert teaches a timer that "automatically deactivates" an application after a predetermined time. Ex-1006, 6:49-52. A POSITA would have recognized that such a timer would ensure that the application is *automatically deactivated*. Ex-1003, pp. 59-60.

In light of Deibert's teachings, it would have been obvious to a POSITA for Brand's authentication application to use a timer that automatically deactivates the authentication application after the authentication server receives a result that confirms or denies the transaction. Ex-1003, p. 60. This is because once the authentication server receives the result, the authentication application has fulfilled its purpose which is authenticating the user to a transaction. Ex-1003, p. 60. While the authentication application could deactivate immediately, a POSITA would have recognized that a user might perceive the sudden deactivation of the application as an abnormal termination (i.e., a "crash") of the application. Thus, a

POSITA would have found it obvious for the authentication application to remain active for a short period of time so that it can provide a completion message to the user (e.g., "Authentication response successfully sent. This application will now close."). Ex-1003, p. 60. A POSITA would have recognized that Deibert's deactivation timer would allow for this form of user interface feature, which improves the user's interaction with the authentication application. Ex-1003, p. 60. Deactivating the authentication application automatically would make the authentication application easier to use because the application is deactivated without user intervention, freeing up resources of the mobile device. Ex-1003, p. 60. *See* Reasons to Combine Brand and Deibert, § IX.C.5.

Accordingly, Brand and Deibert teach a timer that sets a predetermined timeout time to deactivate an authentication application after the authentication server receives a result, which renders obvious "*thereafter ensuring that the authentication function is automatically deactivated*." Ex-1003, p. 60.

D. Ground #1: Claims 14, 21, and 24-26 are obvious over Brand, Williams, Deibert, and Rahman.

1. Rahman

Rahman generally relates to mobile stations with subscriber identities for establishing "wireless communication" with multiple networks. Ex-1011, 3:6-14.

Rahman also teaches a mobile station that includes a "transceiver (XCVR)," a "microprocessor," and a "speaker." Ex-1011, 17:5, 17:61-63, 16:61-63. The mobile station includes physical or user interface elements, e.g. keypad, stylus, touch sensitive display, for "user input selections." Ex-1011, 17:49-59.

2. Reasons to Combine Brand and Rahman

A POSITA would have found it obvious to combine the teachings of Brand with Rahman for multiple reasons, including to obtain the obvious, beneficial, and predictable results of transmitting data in a wireless network, providing a user-friendly interface, executing applications, and issuing audible alerts. Ex-1003, ¶ 148.

As an initial matter, a POSITA when considering the teachings of Brand would have also considered the teachings of Rahman, as they are analogous art with both describing mobile communication systems. Ex-1005, 6:53-64, 7:3-15; Ex-1011, 16:52-18-33; Ex-1003, ¶ 149.

a) A transceiver for wireless communication.

Brand teaches a mobile device that communicates over a "two-way communication network." Ex-1005, 5:65-6:3. A POSITA would have recognized that a mobile device requires a component for communicating over a two-way communication network. Ex-1003, ¶ 152.

Rahman teaches a wireless device, *e.g.*, a smartphone or a handset that includes a transceiver for "two-way wireless communication" in a GSM network. Ex-1011, 16:55-59.

It would have been obvious to a POSITA for Brand's mobile device to include a wireless transceiver. Ex-1003, ¶ 154. A transceiver would beneficially allow a user to communicate over a wireless network, such as a GSM network taught in both Brand and Rahman. Ex-1003, ¶ 154; Ex-1005, 5:67, 6:53-64, 7:3-15; Ex-1011, 17:7-10.

Combining Rahman's wireless transceiver with Brand's mobile device would have been predictable and there would have been reasonable expectation of success. Ex-1003, ¶ 155. Wireless transceivers were a conventional and preferred way for communicating with mobile devices over a wireless network. Ex-1013, 14:25-29; Ex-1017, 2:20-25; *see also* Ex-1005, 5:65-6:3; Ex-1011, 17:7-10; Ex-1003, ¶ 155.

b) A user-friendly interface for initiating applications.

Brand teaches a user who "initiates the authentication application on his/her mobile phone." Ex-1005, 6:53-54. A POSITA would have recognized that initiating an application via a user-interface would be desirable. Ex-1003, ¶ 156.

Rahman teaches a wireless device that includes user interface elements, such as a keypad, stylus, and display for "user input selections." Ex-1011, 17:48-59.

In light of Rahman's teachings, it would have been obvious to a POSITA for Brand's mobile device to include one or more user interface elements. Ex-1003, ¶ 158. Doing so would beneficially provide a user with a user-friendly interface for issuing instructions that initiate and manipulate applications available on (or through) the mobile device. Ex-1003, ¶ 158.

Combining the elements in Rahman's mobile device would have been predictable and a POSITA would have had to a reasonable expectation of success. Ex-1003, ¶ 159. A POSITA would have known that mobile devices commonly included elements to receive user input and trigger an action in response to the input. Ex-1003, ¶ 159; *See* Ex-1013, 40:43-53.

Further, the combination is simply the use of prior art elements (Rahman's user interface element with Brand's mobile device), according to known techniques (software that is responsive to user input) to yield predictable results (initiating an application). Ex-1003, ¶ 160. Such a combination would have been easily accomplished using software programmed to initiate an application in response to a user pressing a key or a button, touching a touchscreen, etc., which would have been within the skill level of a POSITA and predictable. Ex-1003, ¶ 160.

c) An electronic processor for executing the authentication application.

Brand teaches an authentication application that is "running in the Java Virtual Machine (JVM) runtime environment" included in the mobile device. Ex-1005, 9:40-46. A POSITA would have recognized that an electronic processor would run an application. Ex-1003, ¶ 161.

Rahman teaches a microprocessor that "serves as a programmable controller for the wireless device" and "controls all operations of the wireless device 100 in accord with programming that it executes," e.g. applications. Ex-1011, 17:60-63, 18:11-16; *see also id.* 19:15-17.

In view of Rahman's teachings, it would have been obvious to a POSITA for a microprocessor in Brand's mobile device to execute an authentication application. Ex-1003, ¶ 163. It was known for a microprocessor to execute an application to perform tasks. Ex-1003, ¶ 163. Further, an application is written using software code (e.g. Java, C++, or Perl) is conventionally executed with a microprocessor. Ex-1003, ¶ 163; *see also* Ex-1007, 10:47-51.

Further, the combination is simply the use of prior art elements (Rahman's microprocessor and Brand's authentication application), according to known methods (a microprocessor executing software code) to yield predictable results (executing an authentication application). Ex-1003, ¶ 164.

d) A body to protect the internal components of the mobile device

Brand teaches a mobile device with a housing. Ex-1005, Figure 1. A POSITA would have recognized that a housing for protecting the internal components of a mobile device would be desirable. Ex-1003, ¶ 165.

Rahman teaches a housing that surrounds a microprocessor, transceiver, and memory of the mobile device. Ex-1011, Figure 5.

It would have been obvious to a POSITA for a microprocessor (and other components) to be inside the housing of a mobile device and thus protected from damage caused by environment, a user, and ordinary wear-and-tear. Ex-1003, ¶ 167; *see* Ex-1013, 14:4-10, 17:49-52 (describing a cellular telephone with a processor "supported by an external housing").

The combination is simply combining prior art elements (Rahman's housing and Brand's mobile device), according to known methods (packaging device components within a housing) to yield predictable results (protecting the components). Ex-1003, ¶ 168.

e) A mobile device that includes multiple mobile addresses for connecting to wireless networks that use different technologies

First, Brand teaches a communication link "established between the server and the transacting user's mobile communication device." Ex-1005, 4:3-5. The link can be a "GSM or CDMA communications link." Ex-1005, 4:57-60. A POSITA would have recognized that GSM and CDMA networks have different underlying

technologies and for a mobile device cannot operate in both unless the device is compatible with both technologies. Ex-1003, ¶ 169. A POSITA would have recognized that a mobile device that operates in CDMA and GSM networks is desirable because a user would have coverage in areas covered by only GSM or CDMA. A user would also be able to use a single mobile device that connects to both networks. Ex-1003, ¶ 170.

Brand further teaches that "the International Mobile Subscriber Identity (IMSI) number of the SIM card [is] assigned to the user and used in the mobile phone." Ex-1005, 6:9-11. A POSITA would have recognized that the IMSI is a mobile address because it identifies a mobile device in the GSM network. Ex-1003, ¶ 171. The CDMA network does not use a SIM card or an IMSI number to identify a mobile device. Ex-1003, ¶ 171. Instead, the CDMA network identifies a mobile device using a mobile identification number (MIN) that can be programmed into the device. Ex-1003, ¶ 171. A MIN is also a mobile address. Ex-1003, ¶ 171. Because GSM uses IMSI and CDMA uses MIN to identify the mobile device, a POSITA would have recognized that a mobile device would need two addresses to function in GSM and CDMA networks. Ex-1003, ¶ 171.

Rahman teaches multiple "subscriber identifiers of the mobile station." Ex-1011, 3:18-20. The subscriber identity is "represented by an IMSI" or "by an

Mobile Directory Number and Mobile Identification Number pair (MDN/MIN) pair." Ex-1011, 4:37-48, 4:5-8.

In view of Rahman's teachings, it would have been obvious for Brand's mobile device to have multiple mobile addresses to connect to networks that use different technologies, *e.g.*, CDMA and GSM. Ex-1003, ¶ 173. In this way, the mobile device would have coverage in locations covered by only a CDMA or GSM network. Ex-1003, ¶ 173. This would allow the user greater access to Brand's authentication system. Ex-1003, ¶ 173.

Second, Brand's mobile device establishes a communication link over a GSM or CDMA network. Ex-1005, 4:57-60. A POSITA would have recognized that to establish a communication link, the mobile device would first register with the network by authenticating its IMSI or MIN number. Ex-1003, ¶ 174.

Rahman teaches that "once the network has been selected, the mobile station selects the identity associated with the selected network." Ex-1011, 7:30-32. "The mobile station will then use the selected identity to register the mobile device with the selected network... to avail itself of wireless communication services." Ex-1011, 7:32-35.

In light of Rahman's teachings, it would have been obvious to a POSITA that Brand's mobile device would register with the networks. Ex-1003, ¶ 176. Once registered, the mobile device would be able to use the "wireless

communication services" of the network, including establishing a wireless communication link between the mobile device and the authentication server for authentication. Ex-1011, 7:32-35; Ex-1005, 6:60-64; Ex-1003, ¶ 176.

Third, as discussed at IX.D.2.b, it would have been obvious to a POSITA for Brand's mobile device to receive user input using a keyboard, touchscreen display, etc. Ex-1003, ¶ 177. Rahman teaches that an element receives "user input of selections... during mobile subscriber identity operation." Ex-1011, 17:48-53. A POSITA would have recognized that user input during subscriber identity selection would select a mobile device's network. Ex-1003, ¶ 177. This beneficially allows a user to choose a network among the available networks and select a network with favorable call or text messaging rates, quality of service, and/or domestic and international roaming charges. Ex-1003, ¶ 177.

Fourth, as discussed above, it would have been obvious to a POSITA for Brand's mobile device to store multiple mobile addresses to connect to multiple networks. Ex-1003, ¶ 178. POSITA would have also recognized that it is also desirable for the mobile device to automatically select a wireless network and the corresponding subscriber identity to register the mobile device with the network. Ex-1003, ¶ 178. This would make the mobile device easier to use because an algorithm would be able to select a desirable wireless network. Ex-1003, ¶ 178.

Rahman teaches "an identity selection algorithm, which selects a subscriber identity of the mobile station." Ex-1011, 6:16-17. It would have been obvious to a POSITA to select a subscriber identity using an algorithm to provide a flexible approach to connecting to a corresponding wireless network. Ex-1003, ¶ 179. In this way, the algorithm can automatically select an optimal subscriber identity which is used to connect to the wireless network based on pre-programmed criteria. Ex-1003, ¶ 179. Further, using an algorithm to select a subscriber identity would be cost effective because an algorithm would be able to evaluate the cost of operating the mobile device in different networks and select a cost-effective network. Ex-1003, ¶ 179.

f) An acoustic transducer for issuing notifications.

Brand teaches a mobile device that includes "an appropriate alarm to attract the users (9) attention." Ex-1005, 7:6-8. Such alarms were known to be desirable and were common used. Ex-1003, ¶ 180; Ex-1007, 8:16-17.

Rahman teaches a mobile device with a speaker "for audio signal output." Ex-1011, 16:61-63.

It would have been obvious to a POSITA for Brand's mobile device to have a speaker for issuing an audible alarm. A speaker would make the mobile device easier to use because an audible alarm would notify a user of an event, even if the

user was not looking at or interacting with the mobile device at the time of the event. Ex-1003, ¶ 182.

A POSITA would have also recognized that a mobile device emitting an alarm would benefit Brand's authentication system. Ex-1003, ¶ 183. A POSITA would have recognized that a mobile device issuing an audible alarm when the authentication application has successfully initiated is desirable because the alarm would indicate that the authentication application is active. Ex-1003, ¶ 183. This is beneficial because a user is notified that a communication link with the authentication server was established and the mobile device is ready to receive a request to confirm a transaction. Ex-1003, ¶ 183.

Further, the combination is simply combining prior art elements (Rahman's audio signal output with Brand's mobile device), according to known method (audio output via a speaker) to yield predictable results (issuing an audible alert when the application is initialized). Ex-1003, ¶ 184. Further, the combination would have had a reasonable expectation of success, because mobile devices routinely included speakers that issued audible alerts. Ex-1003, ¶ 184; Ex-1016, Figure 1, 7:14-17, 7:30-31.

3. Reasons to Combine Brand, Deibert, and Rahman

As discussed in IX.C.5, Brand and Deibert render obvious automatically deactivating Brand's authentication application. Ex-1003, ¶ 186.

As discussed in IX.D.2.f, Brand and Rahman render obvious generating an audible alert using a speaker. Ex-1003, ¶ 187.

It would have been obvious to a POSITA for Brand's mobile device to issue an audible alert when the authentication application deactivates. Ex-1003, ¶ 188. An audible alert would have been desirable because it would beneficially inform the user that the application has successfully deactivated. Ex-1003, ¶ 188. This would beneficially notify the user that the application will not receive further messages that prompt the user to authenticate a transaction. Ex-1003, ¶ 188.

Further, the combination is simply combining prior art elements (Rahman's audio signal output and Brand and Deibert's application deactivation), according to known methods (audio output via a speaker) to yield predictable results (alerting the user). Ex-1003, ¶ 189.

4. Claim 14

[14.0] A mobile device for use with the authentication method according to claim 1, comprising:

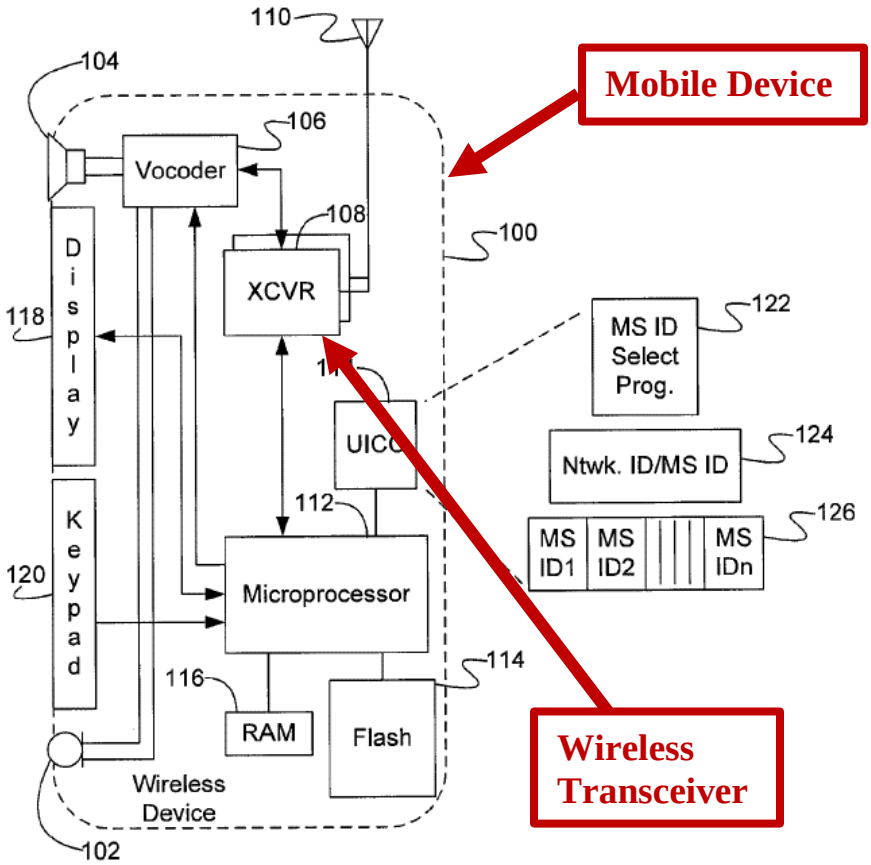
See analysis at [10.0]-[10.1]. Ex-1003, p. 127.

[14.1] a wireless transceiver,

Brand and Rahman render this limitation obvious. First, Brand discloses that a mobile device communicates "via a GSM network." Ex-1005, 5:65-67. Brand discloses that an authentication application executing in a mobile device receives "a transaction confirmation request" and sends a "result." Ex-1005, 7:3-5, 7:12-13,

7:25-27. Accordingly, Brand discloses that the mobile device sends and receives messages.

Second, Rahman, which like Brand describes mobile devices, teaches a mobile device with "at least one digital transceiver (XCVR)." Ex-1011, 17:4-5. The "**transceiver 108 provides two-way wireless communication of information**," (Ex-1011, 17:18-19) and is illustrated below:



Ex-1011, FIG. 5 (Annotated); Ex-1003, p. 130..

In light of Rahman's teachings, it would have been obvious to a POSITA for Brand's mobile device to use a transceiver for two-way wireless communications

to transmit and receive information over a wireless network. Ex-1003, p. 130. Wireless transceivers were routinely used in mobile devices. Ex-1003, p. 130. *See also* Reasons to Combine Brand and Rahman, § IX.D.2.a.

Accordingly, Brand in combination with Rahman teaches a mobile device with *a wireless transceiver*. Ex-1003, p. 130.

[14.2] an ON-switch and

Brand and Rahman render this limitation obvious. First, Brand discloses a user who "initiates the authentication application on his/her mobile phone." Ex-1005, 6:53-54.

Second, Rahman teaches physical and user interface "**elements**" such as a keypad, stylus and touch sensitive display. Ex-1011, 17:47-48, 17:57-59. The elements may be used for "user input selections." Ex-1011, 17:49-51, *see also id.* 17:53-55.

A POSITA would have recognized that any of the elements taught in Rahman is an *ON-switch*. Ex-1003, p. 131. The specification describes an *ON-switch* as "a button, so that the user may activate the authentication function ... by pressing the button," "an input device for inputting some secret code," or "a biometric sensor" that activates a transceiver acting as an authentication function. Ex-1001, 8:42-49.

It would have been obvious to a POSITA for one of Rahman's user input elements to initiate the authentication application executing on Brand's mobile device. This would provide a user with an easy-to-use user interface for quickly initializing an authentication application when conducting a transaction. Ex-1003, p. 131. Additionally, using a stylus, keypad, or touchscreen display as an *ON-switch* was a well-known technique within the skill set of a POSITA. Ex-1003, pp. 131-132. *See also* Reasons to Combine Brand and Rahman, § IX.D.2.b.

Accordingly, the combination of Brand and Rahman teaches a mobile device with a stylus, a keypad, or a touchscreen display, which renders obvious "*an ON-switch*," as claimed. Ex-1003, p. 132.

[14.3.0] an electronic controller that implements said authentication function and

Brand and Rahman render this limitation obvious. First, as discussed in [1.2], Brand discloses an authentication application (*authentication function*), which "runs in the JVM [Java Virtual Machine] environment" in the mobile device. Ex-1005, 9:40-46.

Second, Rahman teaches a microprocessor (*electronic controller*) that is "a programmable controller" and "controls" (*implements*) "all operations of the wireless device 100 in accord with programming that it executes" including applications. Ex-1011, 17:60-63, 18:11-16; Ex-1003, pp. 132-133.

It would have been obvious to a POSITA for a microprocessor (as in Rahman) to execute Brand's authentication application. This would authenticate a user to a transaction. Ex-1003, p. 133. Also, it was routine for mobile devices to use microprocessors to execute an application. Ex-1003, p. 133. *See also* Reasons to Combine Brand and Rahman, § IX.D.2.c.

Accordingly, the combination of Brand and Rahman teaches a mobile device with a microprocessor that executes an authentication application, which renders obvious this limitation. Ex-1003, p. 133.

[14.3.1] [an electronic controller that…] is configured to activate the authentication function in response to the ON-switch being operated and

Brand and Rahman render this limitation obvious. First, as discussed in [1.2], Brand discloses an authentication application (*authentication function*) that the user "**initiates**... on his/her mobile phone." Ex-1005, 6:53-55.

Second, as discussed in [14.3.0], Brand and Rahman teach a microprocessor (*electronic controller*) that implements the authentication application. Ex-1011, 17:60-63.

Third, as discussed in [14.2], Brand and Rahman teach an *ON-switch* which receives user input (*being operated*) that activates the authentication application. Ex-1003, p. 134.

In light of Rahman's teachings, it would have been obvious to a POSITA that a user interface element would initiate an authentication application in response to user input. This would make the authentication system easier to user by providing a user with a user-friendly interface for initiating the authentication application. Ex-1003, p. 134. *See also* Reasons to Combine Brand and Rahman, § IX.D.2.b.

It would have been obvious to a POSITA that the microprocessor would be "*configured*…" such as through the use of software instructions. Ex-1003, p. 134, Ex-1011, 17:60-18:22.

Accordingly, the combination of Brand and Rahman teaches a microprocessor that activates an authentication application in response to receiving user input via a keypad, stylus, or a touch sensitive display, which renders obvious *"[an electronic controller that…] is configured to activate the authentication function in response to the ON-switch being operated."* Ex-1003, p. 134.

[14.3.2] [an electronic controller that… is configured to…] deactivate the authentication function one of: after it has been active for a predetermined time interval after its state has been checked.

Brand, Deibert, and Rahman render this limitation obvious. First, as discussed in [14.3.0] and [14.3.1], Brand and Rahman render obvious "*an electronic controller that implements said authentication function and is configured to*…," and as discussed in [1.4] and [1.6], Brand and Deibert teach to

deactivate the authentication function. As discussed regarding claim construction, the plain language does not recite the *after* limitations as alternatives.

Second, as discussed in [1.4], Brand discloses *activation* of the *authentication function* when the authentication application is initiated.

Third, as discussed in [1.4], Deibert describes "code relating to a timer that automatically **deactivates** any mobile payment applications **after a predetermined timeout time has elapsed**." Ex-1006, 6:49-53. The predetermined timeout time is *a predetermined time interval*. Ex-1003, p. 135.

For the reasons discussed in [1.5], Brand's disclosure of a result transmitted from the authentication application teaches that the authentication application is *active*. Ex-1003, p. 136. Brand further discloses that the authentication server *checks* that the authentication application is active because the server reads the result and sends a positive or negative "authentication result" to the banking institution server. Ex-1005, 7:8-15, 7:25-29, 8:25-31.

It would have been obvious to a POSITA to use the deactivation code in Deibert to deactivate Brand's authentication application after the authentication server receives and reads a result from the authentication application for the reasons discussed [1.6]. Ex-1003, p. 136. This is because after the authentication server receives the result from the authentication application, the authentication application has fulfilled its purpose in Brand's authentication system. Ex-1003,

¶ 90. Thus, it would have been obvious to present the user with a message indicating that the result had been successfully transmitted and that the authentication application would soon deactivate. Ex-1003, ¶ 90. To provide this functionality, the authentication application would start a deactivation timer after the authentication server receives the result from the authentication application. *See* Reasons to Combine Brand and Deibert, § IX.C.5.

Accordingly, Brand and Deibert teach deactivating the authentication application after a predetermined time period beginning when the authentication result is received, which renders obvious to "*deactivate the authentication function... after it has been active for a predetermined time interval after its state has been checked*." Ex-1003, pp. 134-135.

Alternatively, if the claim language is interpreted as having an "or" inserted between the two "*after*" clauses, then the claim remains obvious over the prior art for the reasons discussed above and in [1.6]. Ex-1003, p. 136. For example, Deibert initiates a "countdown timer" "once the mobile payment application has been executed." Ex-1007, 3:48-51. "If the predetermined timeout time elapses" then "the mobile payment application deactivates." Ex-1007, 3:63-64.

5. Claim 21

[21.0] The device according to claim 14, comprising

See analysis at [14.0]-[14.3.2]. Ex-1003, p. 136.

[21.1] a body that encapsulates at least the controller and prevents access thereto.

Brand and Rahman render this limitation obvious. First, as discussed in [14.0], Brand discloses a *mobile device*. Brand further discloses a mobile device that has a housing (*body*):

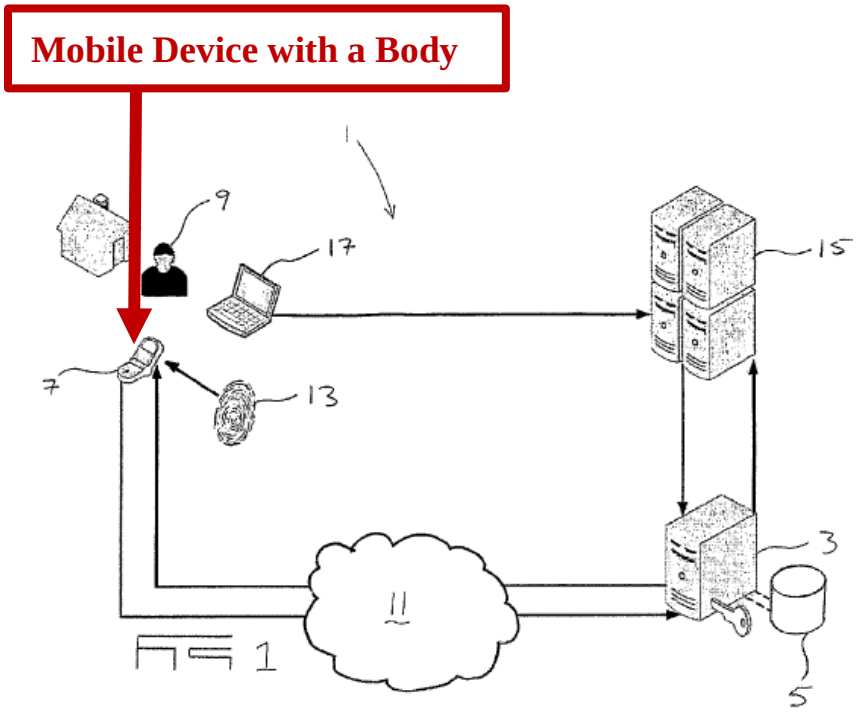


FIG. 1 (Annotated); Ex-1003, p. 137.

Second, as illustrated in Figure 4, Rahman also teaches that mobile devices 12, 13, and 33 each have a housing (*body*).

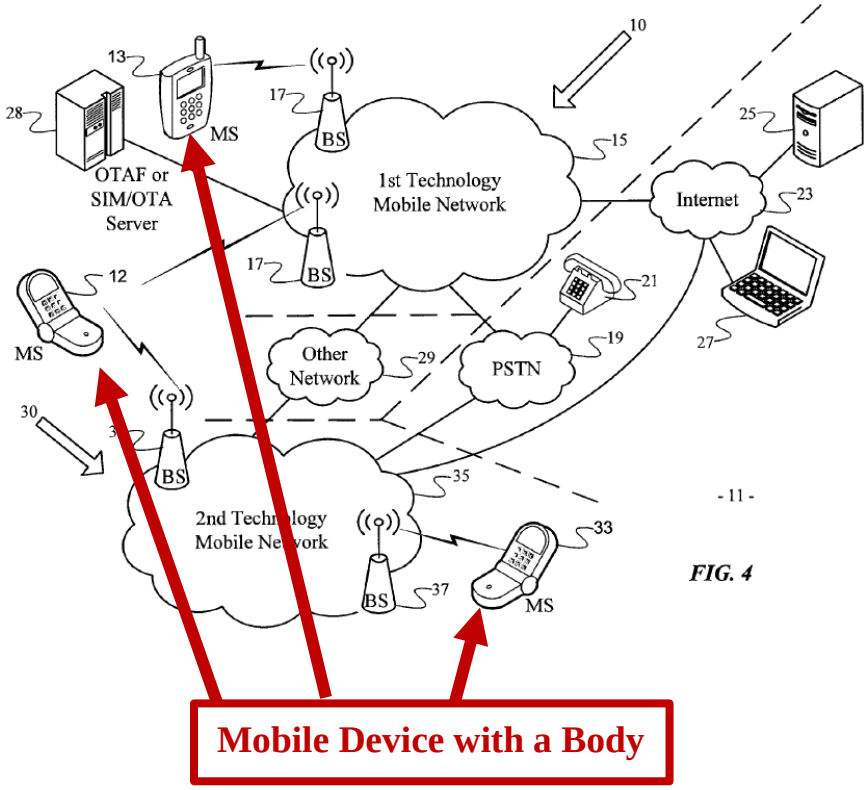


FIG. 4 (Annotated); Ex-1003, p. 138.

As illustrated in Figure 5, Rahman teaches that the housing *encapsulates* the microprocessor, transceiver, and Flash/RAM memories (*at least the controller*) inside the mobile device:

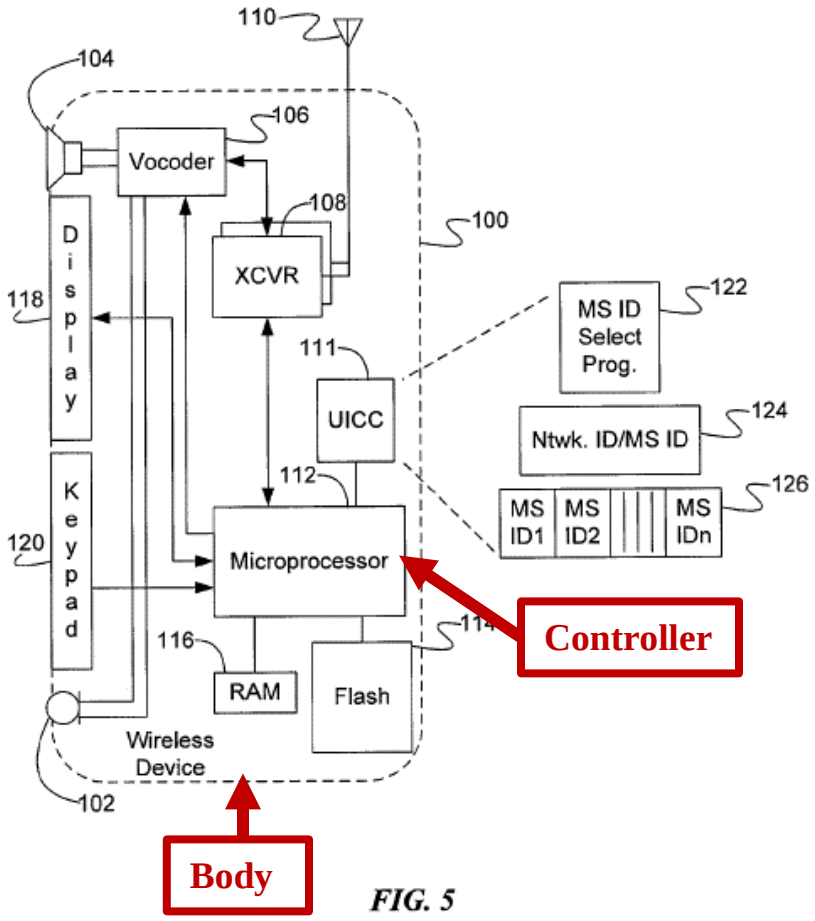


FIG. 5 (Annotated); Ex-1003, p. 139

A POSITA would have recognized that encapsulating a microprocessor and other components inside the housing of the mobile device would *prevent[] access* to these components. Ex-1003, p. 139.

It would also have been obvious to a POSITA for a microprocessor (and other components) to be inside the body of Brand's mobile device. Ex-1003, p. 139. The body would protect the components from external elements, such as water, heat, etc., that could damage them. Ex-1003, p. 139. Also, it would have been obvious to a POSITA for the microprocessor and other components be inside

the body of the mobile device to deter an unauthorized user from obtaining easy access to the components. Ex-1003, pp. 139-140. *See also* Reasons to Combine Brand and Rahman, § IX.D.2.d.

Accordingly, the combination of Brand and Rahman teaches a microprocessor, transceiver, and memory that are included inside a housing of a mobile device, which renders obvious "*a body that encapsulates at least the controller and prevents access thereto*." Ex-1003, p. 140.

6. Claim 24

[24.0] The device according to claim 14, comprising

See analysis at [14.0]-[14.3.2]. Ex-1003, p. 140.

[24.1] a storage for a plurality of mobile addresses,

Brand and Rahman render this limitation obvious. First, as discussed in [14.1], Brand discloses a *mobile device*.

Second, Brand discloses that "**a mobile phone memory normally includes designated *storage* areas.**" Ex-1005, 9:37-38.

Third, Rahman also teaches "**subscriber identifiers** of the mobile station stored in **memory of the mobile station**." Ex-1011, 3:18-21. Rahman further teaches that the subscriber identities are "represented by an IMSI" or "by an Mobile Directory Number and Mobile Identification Number pair (MDN/MIN)." Ex-1011, 4:1-2, 4:5-8; *see id.* 6:9-11.

As discussed in IX.D.2.f, a POSITA would have recognized that the IMSI, MDN, and MIN are examples of *mobile addresses* because they identify the address of a mobile device in a particular network. Ex-1003, p. 141. The specification describes a mobile telephone number as an example of a mobile address. *See* Ex-1001, 3:1-2, 4:55. Ex-1003, pp. 141-142.

It would have been obvious to a POSITA to store subscriber identities in a memory storage of Brand's mobile device. Ex-1003, p. 142. This would beneficially allow the mobile device to connect and operate in wireless networks, such as GSM and CDMA networks that use different subscriber identifiers and allow a user better access to the authentication system in areas covered by GSM or CDMA network. Ex-1003, p. 142. *See also* Reasons to Combine Brand and Rahman, § IX.D.2.e.

Accordingly, the combination of Brand and Rahman teaches a storage in the mobile device that stores subscriber identities, which renders obvious this limitation. Ex-1003, p. 142.

[24.2] and an input including the ON-switch and

See analysis at [14.2]-[14.3.1]. Ex-1003, p. 142.

[24.3] [an input] adapted to selectively activate one of a plurality of authentication functions each of which is assigned to a different one of said mobile addresses.

Brand and Rahman render this limitation obvious. First, as discussed in [24.1], Rahman teaches using multiple subscriber identities (*plurality of mobile addresses*).

Second, Rahman teaches multiple networks supporting "3GPP2 (1xRTT, EVDO)" and "3GPP (LTE/GSM/UMTS) access technologies." Ex-1011, 5:64-66. Rahman teaches that a subscriber identity "must be selected to register the mobile station with the selected network." Ex-1011, 7:26-27. "The mobile station will then use the selected identity to register the mobile device with the selected network." Ex-1011, 7:32-35. A POSITA would have recognized that the registration process between the mobile device with the wireless network authenticates the mobile device to the network and is *an authentication function*. Ex-1003, p. 143. Thus, the registration processes between the mobile device and multiple wireless networks teach "*a plurality of authentication functions*." Ex-1003, p. 143. Further, because the mobile station will "use the selected identity to register the mobile device with the selected network," Rahman teaches that each authentication function *is assigned to a different one of said mobile addresses*. Ex-1011, 7:32-35; Ex-1003, p. 143.

It would have been obvious to a POSITA for Brand's mobile device to register with a selected wireless network using the subscriber identity assigned to that network, as described in Rahman. Ex-1003, p. 143. Registration with the wireless network would beneficially provide the mobile device with wireless communication services associated with the network, including establishing a communication link to the authentication server that authenticates a user to a transaction. Ex-1003, p. 143. *See also* Reasons to Combine Brand and Rahman, § IX.D.2.e.

Third, Rahman teaches an element (*ON-switch*) which receives "user input of selections ... during mobile subscriber identity operation." Ex-1011, 17:48-53. A POSITA would have recognized that the user *input* selections can select a wireless network. Ex-1003, p. 144. The mobile device would then match the *input* with a corresponding subscriber identity "to register the mobile device with the selected network" which teaches *input adapted to selectively activate one of a plurality authentication functions*. Ex-1011, 7:32-35; Ex-1003, p. 144.

It would have been obvious to a POSITA that the mobile device in Brand would receive user *input* that selects a wireless network and causes the mobile device to register with the network as taught in Rahman. This would provide a user with a flexible approach for selecting a favorable wireless network. Ex-1003, p.

144; Ex-1011, 14:32-37. *See also* Reasons to Combine Brand and Rahman, § IX.D.2.e.

Accordingly, Brand combined with Rahman teaches receiving a user input that selects a wireless network that the mobile device matches with the subscriber identity to register the mobile device with the selected network, which renders obvious an input "*adapted to selectively activate one of a plurality of authentication functions each of which is assigned to a different one of said mobile addresses*". Ex-1003, p. 144.

7. Claim 25

[25.0] The device according to claim 14, comprising

See analysis at [14.0]-[14.3.2]. Ex-1003, p. 145.

[25.1] a storage for a plurality of mobile addresses,

See analysis at [24.1]. Ex-1003, p. 145.

[25.2] wherein the controller is configured to select one out of the plurality of mobile addresses according to a predetermined algorithm.

Brand and Rahman render this limitation obvious. First, as discussed in [14.3.0] and [14.3.1], Rahman teaches a microprocessor (*controller*) *configured* to perform operations on the mobile device, and as discussed in [24.1] Rahman teaches subscriber identities (*plurality of mobile addresses*). Ex-1003, p. 145.

Second, Rahman teaches a "mobile station having **multiple subscriber identities ... utilizes an identity selection algorithm**, which **selects a subscriber**

identity of the mobile station." Ex-1011, 6:12-18. Rahman also teaches example algorithms that select a subscriber identity based on "network selected for wireless communications." Ex-1011, 11:5-11, 6:18-19.

In light of Rahman's teachings, it would have been obvious to a POSITA to use an algorithm that selects a mobile address for Brand's mobile device to connect to a wireless network. Ex-1003, p. 146. Using an algorithm would make the mobile device easier to use because an algorithm would automatically select a mobile address to connect the mobile device to a favorable wireless network. Ex-1003, p. 146. *See also* Reasons to Combine Brand and Rahman, § IX.D.2.e.

Accordingly, the combination of Brand and Rahman teaches a microprocessor in the mobile device that uses an algorithm to select from among different subscriber identities, which renders obvious this limitation. Ex-1003, p. 146.

8. Claim 26

[26.0] The device according to claim 14, comprising

See analysis at [14.0]-[14.3.2]. Ex-1003, p. 146.

[26.1] an acoustic transducer for providing an acoustic feedback signal

Brand and Rahman render this limitation obvious. First, Brand discloses that the authentication application "triggers... **an appropriate alarm** to attract the users

(9) attention." Ex-1005, 7:6-8. A POSITA would have recognized the desirability of a speaker that generates an alarm. Ex-1003, p. 147.

Second, Rahman teaches a wireless device that includes "**a speaker 104 for audio signal output**." Ex-1011, 16:52-54; 16:61-63. A speaker is an *acoustic transducer* and the audio signal output that the speaker *provide[s]* is *an acoustic feedback signal*. Ex-1016, 9:64; Ex-1003, p. 147.

In light of Rahman's teachings, it would have been obvious to a POSITA that a speaker in Brand's mobile device would emit an audio signal to alert a user. Ex-1003, pp. 147-148. Audio signals "provide further information to the user." Ex-1012, ¶ 88. In the authentication system, an audio signal would beneficially alert the user that the authentication application has successfully activated or deactivated. Ex-1003, p. 148. *See also* Reasons to Combine Brand and Rahman, § IX.D.2.f.

Accordingly, the combination of Brand and Rahman teaches a mobile device that includes a speaker that emits an audio signal, which renders obvious this limitation. Ex-1003, p. 148.

[26.2] [providing an acoustic feedback signal] upon at least one of activation ... of the authentication function.

As discussed in the claim construction section, the language in [26.2] and [26.3] recites two alternative limitations. The prior art renders both limitations obvious. Ex-1003, p. 148.

First, as discussed in [1.4], Brand discloses that the user "initiates the authentication application" (*activation of the authentication function*). Ex-1005, 6:53-55. As discussed in [26.1], Brand and Rahman teach a mobile device that emits an alert (*acoustic feedback signal*).

It would have been obvious to a POSITA for Brand's mobile device to generate an audible alert as taught in Rahman upon activation of the authentication application. Ex-1003, p. 148. This would notify the user that the authentication application was successfully activated and is about to receive a request for a user to confirm a transaction. Ex-1003, p. 148. Issuing an alert that an application was activated was technique known to a POSITA. Ex-1003, p. 148; *see also* Ex-1007, 8:10-18, 8:52-56. *See also* Reasons to Combine Brand and Rahman, § IX.D.2.f.

Accordingly, the combination of Brand and Rahman teaches a mobile device that issues an alert when an authentication application is activated, which renders this limitation obvious. Ex-1003, p. 149.

[26.3] [providing an acoustic feedback signal] upon at least one of ... deactivation of the authentication function.

Brand, Deibert, and Rahman render this limitation obvious. As discussed in [1.6], Brand and Deibert render obvious *deactivat[ing]* the authentication function and as discussed in [26.2], Brand and Rahman teach a speaker generating an audio signal output (*acoustic feedback signal*).

It would have been obvious to a POSITA for Brand's mobile device to emit an audio signal when the authentication application is deactivated as taught in Deibert because it would notify the user that the authentication application has successfully deactivated. Ex-1003, p. 149; *See also* Reasons to Combine Brand, Deibert, and Rahman, § IX.D.3 and Reasons to Combine Brand and Rahman, § IX.D.2.f.

Accordingly, the combination of Brand, Deibert, and Rahman teaches a mobile device that issues an audio signal when an authentication application is deactivated, which renders obvious this limitation Ex-1003, p. 149.

E. Ground #2: Claims 15-17 are obvious over Brand, Williams, Deibert, Rahman, and Partovi.

1. Partovi

Partovi generally relates to charging techniques. Ex-1012, Abstract. Partovi teaches that "mobile devices incorporate rechargeable batteries" and charging the mobile devices "through ... USB or mini usb connector." Ex-1012, ¶¶ 66, 69.

2. Reasons to Combine Brand and Partovi

A POSITA would have found it obvious to combine the teachings of Brand with Partovi for multiple reasons, including to obtain the obvious, beneficial, and predictable result of providing power to Brand's mobile device. Ex-1003, ¶ 194.

As an initial matter, a POSITA when considering the teachings of Brand would have also considered the teachings of Partovi, because both references describe mobile devices. Ex-1005, 6:53-64, 7:3-15; Ex-1012, Abstract; Ex-1003, ¶ 195.

a) Rechargeable battery

Brand teaches a mobile device that operates an authentication application. Ex-1005, 6:53-54, 6:62-64. A POSITA would have recognized that the mobile device requires power to operate, but because the mobile device is "mobile" it should not depend on a stationary power sources. Ex-1003, ¶ 197. Accordingly, a mobile device with a battery that can power the device in a mobile setting (*i.e.*, as the user carries the mobile device) is desirable. Ex-1003, ¶ 197.

Partovi teaches mobile devices with "rechargeable batteries." Ex-1012, ¶ 66.

In light of Partovi's teachings, it would have been obvious to a POSITA for Brand's mobile device to use a rechargeable battery to operate without being connected to a stationary power source. Ex-1003, ¶ 199. Partovi teaches that rechargeable batteries are required "for operation" of the mobile device. Ex-1012, ¶

66. A rechargeable mobile device would beneficially allow the user to authenticate a transaction initiated at the terminal without requiring a stationary power source, *e.g.*, an electrical wall outlet. Ex-1005, 6:53-55, 7:3-15.

Using a rechargeable battery also "sav[es] the user the cost and inconvenience of regularly having to purchase new [battery] cells." Ex-1018, 1:27-30. Recharging a battery is also good for environment. Ex-1003, ¶ 200.

Using a rechargeable battery in Brand's mobile device would have been predictable and there would have been reasonable expectation of success. This is because a rechargeable battery was a conventional and known way to power the mobile device, and a variety of "wired" or "wireless" techniques to recharge the battery in the mobile device were known and available to a POSITA. Ex-1012, ¶¶ 39-42, 54, 67; Ex-1003, 201.

b) Connector

A POSITA would have recognized that charging a rechargeable battery requires a connection to a power source. Ex-1003, ¶ 202.

Partovi teaches an "AC/DC adaptor, USB or mini usb connector" for "charging and/or powering of the mobile device" and its battery from a power source. Ex-1012, ¶ 69; *see also id.* ¶ 39.

It would have been obvious to a POSITA for Brand's mobile device to include a connector for charging the battery because "rechargeable batteries… require external DC power to charge." Ex-1012, ¶ 66; Ex-1003, ¶ 204.

The combination simply uses prior art elements (Partovi's connector and Brand's mobile device), according to known methods (coupling a device to a power source) to yield predictable results (recharging a battery). Ex-1003, ¶ 205. The results would have been predictable because a POSITA would have been familiar with the common use of rechargeable batteries in mobile devices and various charging techniques. Ex-1012, ¶¶ 168, 172-173, 182.

Additionally, it would have been obvious to a POSITA to use a USB-type connector. Ex-1003, ¶ 206. USB-type connectors were widely adopted for use in a mobile device, in part because they are small and allow for easy charging from a computer. Ex-1019, 2:54-57, 1:29-33; Ex-1003, ¶ 206.

c) Charge indicator

As discussed in IX.E.2.a, it would have been obvious for Brand's mobile device to use a rechargeable battery. Ex-1003, ¶ 207. A POSITA would have recognized that batteries have limited capacity, so a user would want to track the charge level. Ex-1003, ¶ 207.

Partovi teaches "indicators" and a display screen that displays "state and level of battery charge indicator." Ex-1012, ¶¶ 85-86, 88-89.

It would have been obvious to a POSITA for Brand's mobile device to indicate the state and level of battery charge to provide the user with battery charge information and inform the user when to recharge the mobile device battery, and when charging is occurring or complete. Ex-1012, ¶ 89; Ex-1003, ¶¶ 209-210. This would allow the user to avoid a depleted battery, which might prevent the user from authenticating the transactions. Ex-1003, ¶ 209.

3. Claim 15

[15.0] The device according to claim 14, further comprising:

See analysis at [14.0]-[14.3.2]. Ex-1003, p. 155.

[15.1] a rechargeable battery and

Brand and Partovi render this limitation obvious. First, as discussed in [1.2], Brand discloses a *mobile device*. Ex-1003, p. 156.

Second, Partovi teaches that "**mobile devices incorporate rechargeable batteries**." Ex-1012, ¶ 66.

It would have been obvious to a POSITA for Brand's mobile device to use a rechargeable battery, as taught in Partovi, to function without being connected to a power source. Ex-1003, p. 156. *See also* Reasons to Combine Brand and Partovi, § IX.E.2.a.

Accordingly, the combination of Brand and Partovi teaches *a rechargeable battery*. Ex-1003, p. 156.

[15.2] a connector for connecting the battery to a voltage source.

Brand and Partovi render this limitation obvious. Partovi teaches that "mobile devices incorporate **rechargeable batteries** and require external **DC power** to charge these batteries." Ex-1012, ¶ 66. Partovi further teaches charging a mobile device battery "**through an AC/DC adaptor, USB or mini usb connector, etc.**" Ex-1012, ¶ 69. A DC power adaptor is a *voltage source*, and a USB or mini USB connector is a *connector*. Ex-1003, pp. 156-157.

In light of Partovi's teachings, it would have been obvious to a POSITA for Brand's mobile device to include a connector for connecting a rechargeable battery to a DC power adaptor (or other suitable power source) to recharge the battery. Ex-1003, p. 157. *See also* Reasons to Combine Brand and Partovi, § IX.E.2.b.

Accordingly, the combination of Brand and Partovi teaches a mobile device that includes a connector that connects the rechargeable battery to a DC power, which renders obvious this limitation. Ex-1003, p. 157.

4. Claim 16

[16.0] The device according to claim 15,

See analysis at [15.0]-[15.2]. Ex-1003, p. 158.

[16.1] comprising a display for indicating the charge state of the battery.

Brand and Partovi render this limitation obvious. First, Brand discloses a "**monitor** of the mobile phone," which is *a display*. Ex-1005, 7:6-8; Ex-1003, p. 158.

Second, Partovi teaches a "**mobile device display screen**" that displays "**indicators**" such as a "**state and level of battery charge indicator**" that *indicat[es] the charge state of the battery*. Ex-1012, ¶¶ 88-89.

It would have been obvious to a POSITA to display a battery charge indicator on a monitor of Brand's mobile device because the user would be able to check the display and determine the amount of charge stored in the battery and when the battery need recharging. Ex-1003, pp. 158-159. *See also* Reasons to Combine Brand and Partovi, § IX.E.2.c.

Accordingly, the combination of Brand and Partovi teaches a mobile device with a display that shows a battery charge indicator, which renders obvious this limitation. Ex-1003, p. 159.

5. Claim 17

[17.0] The device according to claim 15,

See analysis at [15.0]-[15.2]. Ex-1003, p. 159.

[17.1] wherein the connector is one of a USB connector and a micro-USB connector.

As discussed in the claim construction section, the language in [17.1] two alternative limitations. Brand and Partovi render obvious both limitations. Ex-1003, p. 159.

First, Partovi teaches a connector that is a "*USB* or mini usb *connector*." Ex-1012, ¶ 69.

Second, a *micro-USB connector* is an obvious variant of a USB connector. Ex-1003, p. 159. Accordingly, Partovi renders obvious a *micro-USB connector*. Ex-1003, p. 159.

It would have been obvious to a POSITA for Brand's mobile device to use a USB connector or its variant to connect a rechargeable battery to a power source. Ex-1003, pp. 159-160. This is because a USB connector is relatively small and would require little space in the mobile device and can connect the mobile device to other computing devices, e.g., a computer or a laptop, for charging. Ex-1003, pp. 159-160. *See also* Reasons to Combine Brand and Partovi, § IX.E.2.b.

Accordingly, the combination of Brand and Partovi teaches a USB connector or its variant that connects a rechargeable battery included in the mobile device to a power source, which renders obvious this limitation. Ex-1003, p. 160.

F. Ground #3: Claim 19 is obvious over Brand, Williams, Deibert, Rahman, and Carter.

1. Carter

Carter generally relates to authenticating transactions with a mobile device. Ex-1008, Abstract. Carter also teaches "[a] standard cellular phone (referred to as MS) with a built-in or connected GPS or equivalent receiver (or other location determining capability)." Carter, ¶ 104;

2. Reasons to Combine Brand and Carter

A POSITA would have been motivated to combine the teachings of Brand with the teachings of Carter to obtain the obvious, beneficial, and predictable result of improving security of the authentication system. Ex-1003, ¶¶ 97, 100.

First, a POSITA would have considered Brand and Carter together, as they are analogous prior art both pertaining to the field of authenticating transactions. Ex-1005, Abstract; Ex-1008, Abstract; Ex-1003, ¶ 98.

Second, Brand describes an authentication technique that relies on a user being "in possession of his/her mobile phone." Ex-1005, 6:18-21. Accordingly, a POSITA would have recognized that techniques that verify that a user indeed possessed the mobile device while authenticating a transaction are desirable. Ex-1003, ¶ 101.

Carter describes improving transaction security by check to see if the mobile device is near to a location" from which a user conducts a transaction. Ex-1008, ¶¶ 46, 309.

It would have been obvious to a POSITA to use Carter's location-checking technique to determine whether Brand's mobile device is proximate to the terminal initiating a transaction. Ex-1003, ¶ 101. This would indicate whether the user at the terminal possessed the mobile device, and thus, whether the transaction is legitimate. Ex-1003, ¶ 101. Checking for device proximity would also prevent a user from mistakenly approving a transaction initiated at a remote terminal (e.g., by a third party). Ex-1003, ¶ 101.

Third, a POSITA would have been motivated to use Carter's effective authentication techniques. Ex-1003, ¶ 102; Ex-1005, 2:3-6, 2:16-18. Carter teaches cheap and existing location techniques, e.g., "a built-in or connected GPS or equivalent receiver (or other location determining capability)" for determining location. Ex-1008, ¶ 104. Carter's inexpensive and already-implemented locating features provide a cost-effective way to improve security. Ex-1003, ¶ 102.

3. Claim 19

[19.0] The device according to claim 14, comprising

See analysis at [14.0]-[14.3.2]. Ex-1003, p. 161.

[19.1] a positioning function for wireless detection of its own position,

Brand and Carter render this limitation obvious. First, as discussed in [1.2], Brand discloses a *mobile device*.

Second, Carter teaches "[a] standard **cellular phone (referred to as MS) with a built-in or connected GPS** ... or other **location determining capability**." Ex-1008, ¶ 104. A POSITA would have recognized that a location determining capability is *a positioning function*, that GPS detects a position *wireless[ly]*, and that a *mobile device* with a "built-in or connected GPS" would detect *its own position*. Ex-1003, p. 162.

It would have been obvious that Brand's mobile device would use a GPS to detect its location as a cost-effective way increase security of the authentication system. Ex-1003, p. 162. Such a modification is simply the combination combining prior art elements (Brand mobile device and Carter's locating technique built into a mobile device) according to known methods (GPS locating) to yield predictable results (determining location of a mobile device). Ex-1003, p. 162. *See also* Reasons to Combine Brand and Carter, § IX.F.2.

Accordingly, the prior art teaches a mobile device able to determine its location using GPS, which renders obvious this limitation. Ex-1003, p. 162.

[19.2] wherein the authentication function includes a function of sending a detected location via the transceiver.

Brand, Rahman, and Carter render this limitation obvious. First, as discussed in [1.2], Brand discloses an authentication application (*authentication function*), which as discussed in [1.3.2] transmits a "result to [authentication] server" over a

GSM network. Ex-1005, 7:6-13, 7:25-27. Accordingly, the authentication application has *a function of sending* data. Ex-1003, p. 163. As discussed in [19.1], the mobile device detects its *location*.

Second, Carter teaches that "security system 7 interfaces with the MS 1 via a standard wireless communications link." Ex-1008, ¶ 120. The security system in Carter is analogous to the authentication server in Brand because both systems authenticate transactions. Ex-1005, 7:1-17; Ex-1008, ¶ 114-115; Ex-1003, p. 163. The security system uses location information, and the "mobile device can be used to provide *location* information." Ex-1008, ¶¶ 352, 65, 52. It would have been obvious that the mobile station sends its location information via the wireless communication link (e.g., GSM network link) because that is Carter's only communication path between the mobile station and the security system. Ex-1008, Fig. 1; Ex-1003, p. 163.

It would have been obvious to a POSITA for Brand's mobile device to determine and transmit its position to the authentication server. Ex-1003, p. 164. Brand's authentication server already confirms (or denies) transactions based the "result" transmitted from the mobile device. Ex-1005, 7:12-15, 7:25-29. Transmitting mobile device's position in addition to the result would make the authentication system more secure because the authentication server would use the

position to confirm that the user is conducting the transaction. Ex-1003, p. 164. *See also* Reasons to Combine Brand and Carter, § IX.F.2.

Third, as discussed in [14.1], Brand and Rahman render obvious a mobile device that includes a *wireless transceiver*. As discussed in IX.D.2.a, it would have been obvious for the location information to be transmitted over a wireless network *via the transceiver*. Ex-1003, p. 165.

Accordingly, the prior art teaches that a mobile device sends its location via a wireless transceiver, which renders obvious this limitation. Ex-1003, p. 165.

G. Ground #4: Claim 22 is obvious over Brand, Williams, Deibert, Rahman, and Russell.

1. Russell

Russell relates to security that "limits the transfer and distribution of personal data." Ex-1013, Abstract.

Russell teaches a portable device (PID) that includes a "self-destruct element 153 that destroys the identity data if unauthorized access to the stored identity data is attempted." Ex-1013, 16:67-17:2.

2. Reasons to combine Brand and Russell

A POSITA would have been motivated to combine the teachings of Brand and Russell to protect data. Ex-1003, ¶ 217.

A POSITA would have considered Brand and Russell together because they are analogous prior art, with both pertaining to authorizing payment transactions with mobile devices. Ex-1005, Abstract; Ex-1013, 8:1-13. Ex-1003, ¶ 218.

Brand teaches an authentication system that stores a fingerprint "in a secure storage area on the mobile phone." Ex-1005, 6:4-6, 6:12-14, Abstract. The fingerprint "is only readable by authorized software applications" such as Brand's authentication application. Ex-1005, 6:14-16, 6:53-64, 7:3-17. A POSITA would have recognized that if a third-party obtains user's mobile device and stored fingerprint, the third-party would be able to authenticate user's transactions. Ex-1003, ¶ 219. Brand's mobile device also displays "information on the transaction," which may include account number and other identifying information. Ex-1005, 7:6-10; Ex-1003, ¶ 219. Preventing a third-party from accessing the fingerprint and transaction information was have been desirable. Ex-1003, ¶ 219.

Russell teaches a self-destruct element that "destroys the identity data if unauthorized access to the stored identity data is attempted." Ex-1013, 16:67-17:2, 17:3-6.

It would have been obvious to a POSITA for Brand's mobile device to use a self-destruction mechanism to protect data, such as a fingerprint and user information, when an unauthorized third-party attempts to access that data. Ex-1003, ¶ 221. This would contribute to the overall security of the authentication

system because a third-party that obtains the user's mobile device would not be able to access the authentication server to authenticate transactions or otherwise misuse the user identity data. Ex-1003, ¶ 221; Ex-1005, 6:55-64. This would also prevent a third-party from posing as a user and authenticating fraudulent transactions. Ex-1003, ¶ 221.

Such a modification is simply the combination combining prior art elements (Brand mobile device and Russell's self-destruction element) according to known methods to yield predictable results (destroy data). Ex-1003, ¶ 222.

3. Claim 22

[22.0] The device according to claim 14, comprising

See analysis at [14.0]-[14.3.2]. Ex-1003, p. 168.

[22.1] a self-destruction function configured to be activated by an attempt of enforced access.

Brand and Russell render this limitation obvious. First, Brand teaches a unique digital identifier or fingerprint that is "stored in a secure storage area on the mobile phone." Ex-1005, 6:4-6, 6:12-14. Brand also teaches that the authentication application displays "information on the transaction that the user (9) is attempting to perform." Ex-1005, 7:6-10. A POSITA would have recognized that the information may include user identity data, such as account number, username, etc. Ex-1003, p. 169.

Second, Russell teaches a personal identifying device (PID) that includes a "**self-destruct element 153** that **destroys** the identity data if **unauthorized access to the stored identity data is attempted**." Ex-1013, 16:67-17:2. The self-destruct element in a *self-destruction function.* Ex-1003, p. 169. It would have been obvious to a POSITA that the *self-destruction function* is "*configured to be activated*" through the use of software instructions when "**unauthorized *access* to the stored identity data is attempted**." Ex-1013, 7:1-17:2; Ex-1003, pp. 169-170.

It would have been obvious to a POSITA for Brand's mobile device to use a self-destruct element to destroy stored information to prevent a third-party from accessing the information. Ex-1003, p. 170. *See also* Reason to Combine Brand and Partovi, § IX.G.2.

Accordingly, the prior art teaches a self-destruct element that destroys user information if unauthorized access to the data is attempted, which renders obvious this limitation. Ex-1003, p. 170.

X. CONCLUSION

Petitioner requests institution of an *inter partes* review and cancellation of the Challenged Claims.

Respectfully submitted,

Dated: September 24, 2019

/David L. McCombs/

David L. McCombs
Lead Counsel for Petitioner
Registration No. 32,271

HAYNES AND BOONE, LLP
2323 Victory Avenue, Suite 700
Dallas, Texas 75219
Customer No. 27683

CERTIFICATE OF WORD COUNT

Pursuant to 37 C.F.R. §42.24(d), Petitioner hereby certifies, in accordance with and reliance on the word count provided by the word-processing system used to prepare this Petition, that the number of words in this paper is 13,887. Pursuant to 37 C.F.R. §42.24(d), this word count excludes the table of contents, table of authorities, mandatory notices under §42.8, certificate of service, certificate of word count, appendix of exhibits, and any claim listing.

Dated: September 24, 2019

/David L. McCombs/
David L. McCombs
Lead Counsel for Petitioner
Registration No. 32,271

CERTIFICATE OF SERVICE

The undersigned certifies that, in accordance with 37 C.F.R. §42.6(e) and 37 C.F.R. §42.105, service was made on Patent Owner as detailed below.

Date of service	September 24, 2019
Manner of service	FEDERAL EXPRESS
Documents served	Petition for *Inter Partes* Review Under 35 U.S.C. §312 and 37 C.F.R. §42.104 of U.S. 9,246,903; Petitioner's Exhibit List; Exhibits 1001-1008, 1011-1014, 1016-1022, 1024; Petitioner Power of Attorney; and Petitioner's Notice For Filing Multiple Petitions.
Persons served	Richard M. Goldberg 25 East Salem Street, Suite 419 Hackensack, NJ 07601

/David L. McCombs/
David L. McCombs
Lead Counsel for Petitioner
Registration No. 32,271

EXHIBIT D

Trials@uspto.gov
571-272-7822

Paper: 9
Entered: March 27, 2020

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYSTEMS, INC.,
Petitioner,

v.

MONEY AND DATA PROTECTION LIZENZ GMBH & CO. KG,
Patent Owner.

IPR2019-01639
Patent 9,246,903 B2

Before THOMAS L. GIANNETTI, BRYAN F. MOORE, and CHARLES J. BOUDREAU, *Administrative Patent Judges.*

MOORE, *Administrative Patent Judge*.

DECISION
Denying Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

A. Background

Cisco Systems, Inc. ("Petitioner" or "Cisco") filed a Petition requesting *inter partes* review of claims 14–17, 19, 21, 22, and 24–26 (the "challenged claims") of U.S. Patent No. 9,246,903 B2 (Ex. 1001, the "'903 patent"). Paper 3 ("Pet."). Money And Data Protection Lizenz GMBH & CO. KG ("Patent Owner") filed a Preliminary Response. Paper 8 ("Prelim. Resp.").

The standard for institution is set forth in 35 U.S.C. § 314, which provides that an *inter partes* review may not be instituted unless the information presented in the Petition and the Preliminary Response shows that "there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition." 35 U.S.C. § 314; *see also* 37 C.F.R § 42.4(a) ("The Board institutes the trial on behalf of the Director.").

For the reasons that follow, we do not institute *inter partes* review of the challenged claims of the '903 patent.

B. Related Proceedings

The parties identify the following pending district court proceeding involving the '903 patent: *Money and Data Protection Lizenz GmbH & Co. KG v. Duo Security, Inc.,* 1-18-cv-01477 (D. Del.). Pet. 8; Paper 7, 1.

Concurrently with the filing of this Petition, Petitioner also filed a petition challenging certain other claims of the '903 patent in IPR2019-01638. Pursuant to the Trial Practice Guide update dated July 2019, Petitioner has filed a Notice addressing the issue of multiple petitions. Paper 2.

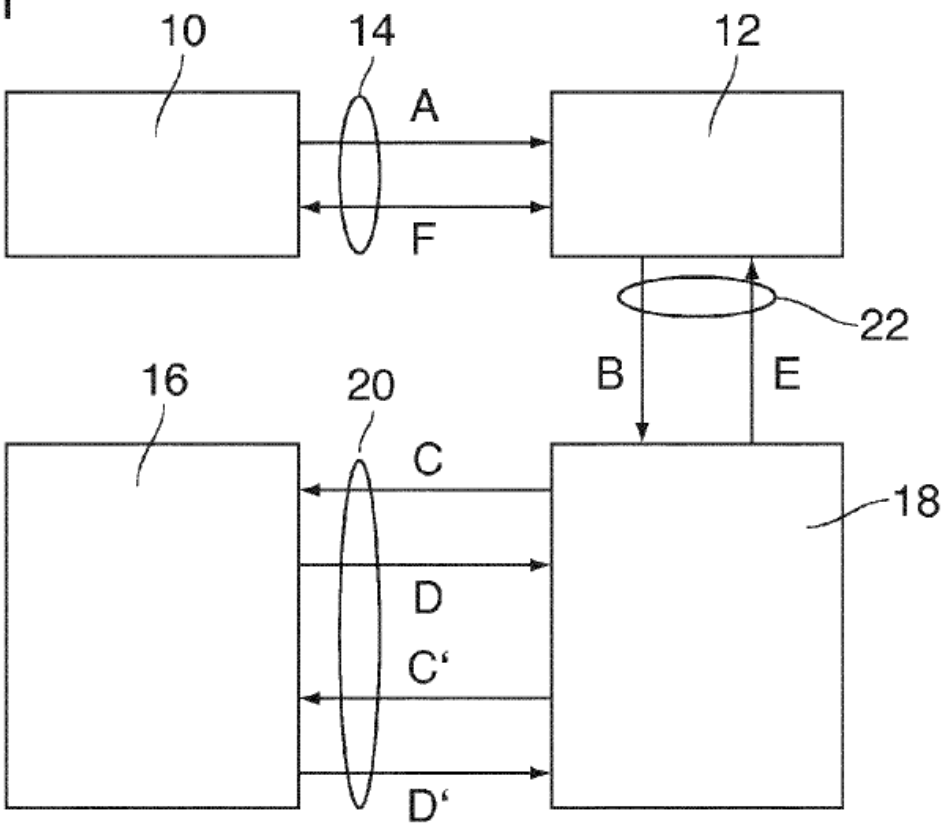
C. Real Parties in Interest

Petitioner identifies "Cisco Systems, Inc. and Duo Security, Inc." as the real parties in interest. Pet. 7. Patent Owner identifies Money and Data Protection Lizenz GmbH & Co. KG, as the real party in interest. Paper 6, 1.

D. The '903 Patent

The '903 Patent describes "authenticating a user to a transaction." Ex. 1001, 1:3–4. The authentication system includes transaction terminal 10, remote transaction partner 12, mobile communication device 16, and authentication device 18. *Id.* at 4:41–45. As illustrated in Fig. 1 below, up to three separate communication channels (14, 20, 22) link the components. *Id.* at 4:39–49.

Fig. 1



As shown in Figure 1, above, a user "operates the terminal 10 and sends a transaction request to the transaction partner 12." *Id.* at 4:57–60; FIG. 1 (A). The request includes a "user-ID." *Id.* at 4:60–61. "[T]he transaction partner 12 forwards the user-ID to the authentication device 18." *Id.* at 4:61–63, FIG. 1 (B). The "authentication device 18 retrieves the mobile telephone number and or the IMSI of the user and contacts the mobile device 16" to check whether an "authentication function . . . is active." *Id.* at 4:63–5:1, FIG. 1 (C). When the authentication device 18 confirms "that the authentication function is active, the authentication device 18 sends an authentication signal to the transaction partner 12." *Id.* at 5:1–3, FIG. 1 (D & E). The authentication signal "informs the transaction partner that this specific user is authenticated to the requested transaction." *Id.* at 5:4–7. The transaction is then "performed via the terminal 10." *Id.* at 5:7–9, FIG. 1 (F).

E. Illustrative Claims

The '903 patent has 26 claims. Seven claims (14–17, 19, 21–22) are challenged in the Petition. *See* Section I.G., *infra.* None of the challenged claims are independent, however, they all depend (directly or indirectly) from claim 1. Additionally, all the challenged claims, except dependent claim 14, also depend (directly or indirectly) from claim 14. Claim 1 recites:

> 1. A method of authenticating a user to a transaction at a terminal, comprising the steps of:
>
> transmitting a user identification from the terminal to a transaction partner via a first communication channel,
>
> providing an authentication step in which an authentication device uses a second communication channel for checking an authentication function that is implemented in a mobile device of the user,

> as a criterion for deciding whether the authentication to the transaction shall be granted or denied, having the authentication device check whether a predetermined time relation exists between the transmission of the user identification and a response from the second communication channel,
>
> ensuring that the authentication function is normally inactive and is activated by the user only preliminarily for the transaction,
>
> ensuring that said response from the second communication channel includes information that the authentication function is active, and
>
> thereafter ensuring that the authentication function is automatically deactivated.

Ex. 1001, 10:39–60.

Claim 14 recites:

> 14. A mobile device for use with the authentication method according to claim 1, comprising:
>
> a wireless transceiver,
>
> an ON-switch and,
>
> an electronic controller that implements said authentication function and is configured to activate the authentication function in response to the ON-switch being operated and to deactivate the authentication function one of: after it has been active for a predetermined time interval after its state has been checked.

Ex. 1001, 10:5–22.

F. References and Other Evidence

The Petition relies on the following references:

1. US 8,862,097 B2, issued Oct. 14, 2014 (filed Dec. 3, 2009) (Ex. 1005, "Brand"),

2. GB 2,398,159 A, published Aug. 11, 2004 (Ex. 1006, "Williams"),

3. US 9,647,855 B2, issued May 9, 2017 (filed Jan. 9, 2008) (Ex. 1007, "Deibert"),

4. US 2011/0202466 A1, published Aug. 18, 2011 (Ex. 1008, "Carter"),

5. U.S. 8,306,532 B2, issued Nov. 6, 2012 (filed June 26, 2009) (Ex. 1011, "Rahman"),

6. US 2011/0050164 A1, published Mar. 3, 2011 (Ex. 1012, "Partovi"), and

7. US 9,659,297 B2, issued Mar. 23, 2017 (filed August 7, 2008) (Ex. 1013, "Russell").

Pet. 12–14.

In addition, Petitioner submits the Declaration of Patrick McDaniel (Ex. 1003, "McDaniel Decl."). Patent Owner has not submitted an expert declaration.

G. Asserted Grounds of Unpatentability

Petitioner asserts the challenged claims are unpatentable on the following grounds.

Claim(s) Challenged	Statutory Basis	References
1	35 U.S.C. § 103	Brand, Williams, and Deibert
14, 21, 24, 25, and 26	35 U.S.C. § 103	Brand, Williams, Deibert, and Rahman
15–17	35 U.S.C. § 103	Brand, Williams, Deibert, Rahman, and Partovi
19	35 U.S.C. § 103	Brand, Williams, Deibert, Rahman, and Carter
22	35 U.S.C. § 103	Brand, Williams, Deibert, Rahman, and Russell

Pet. 13.

II. PRELIMINARY MATTERS

A. Level of Ordinary Skill

Petitioner contends:

> A Person of Ordinary Skill in The Art [] in October 2011 would have had a working knowledge of the authentication art that is pertinent to the '903 Patent, including two-factor authentication using a mobile device. A [person of ordinary skill in the art at the time of the invention] would have had a bachelor's degree in computer science, computer engineering, or an equivalent, and three years of professional experience. Lack of professional experience can be remedied by additional education, and vice versa."

Pet. 10 (citing McDaniel Decl. ¶¶ 15–19). Patent Owner contends: A person of ordinary skill in the art at the time of the invention "would have had a bachelor's degree in computer science, computer engineering, or an equivalent, and two years of work experience." Prelim. Resp. 25. Patent Owner states specifically that it is unnecessary to define the working knowledge of the person of ordinary skill in the art at the time of the invention because by definition a person of ordinary skill in the art is skilled in the art that is relevant to the '903 patent. *Id.*

We do not discern that Petitioner's statement of the "working knowledge" affects the analysis of obviousness in this decision. We do not discern a difference between two or three years of working experience that affects the analysis of obviousness in this decision. We also regard Petitioner's definition as consistent with the prior art before us. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001) (prior art itself may reflect an appropriate level of skill). Thus, for the purpose of our decision, we adopt Petitioner's proposal.

B. Claim Construction

We interpret claim terms using "the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. 282(b)." 37 C.F.R. § 42.100(b) (2019). In this context, claim terms "are

generally given their ordinary and customary meaning" as understood by a person of ordinary skill in the art in question at the time of the invention. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–13 (Fed. Cir. 2005) (citations omitted) (en banc). "In determining the meaning of the disputed claim limitation, we look principally to the intrinsic evidence of record, examining the claim language itself, the written description, and the prosecution history, if in evidence." *DePuy Spine, Inc. v. Medtronic Sofamor Danek, Inc.*, 469 F.3d 1005, 1014 (Fed. Cir. 2006) (citing *Phillips*, 415 F.3d at 1312–17). Extrinsic evidence is "less significant than the intrinsic record in determining 'the legally operative meaning of claim language.'" *Phillips*, 415 F.3d at 1317.

Petitioner requests that we construe several terms (in claims 14, 17, and 26) with language that, according to Petitioner "recite quasi-Markush terms." *Id.* at 11–12. Patent Owner does not argue that the patentability of any claim turns on the construction for any of the above terms. See generally Prelim. Resp. Additionally, issues related to claim 1 are dispositive of this decision. Thus, we see no need to construe any terms for the purposes of this decision.

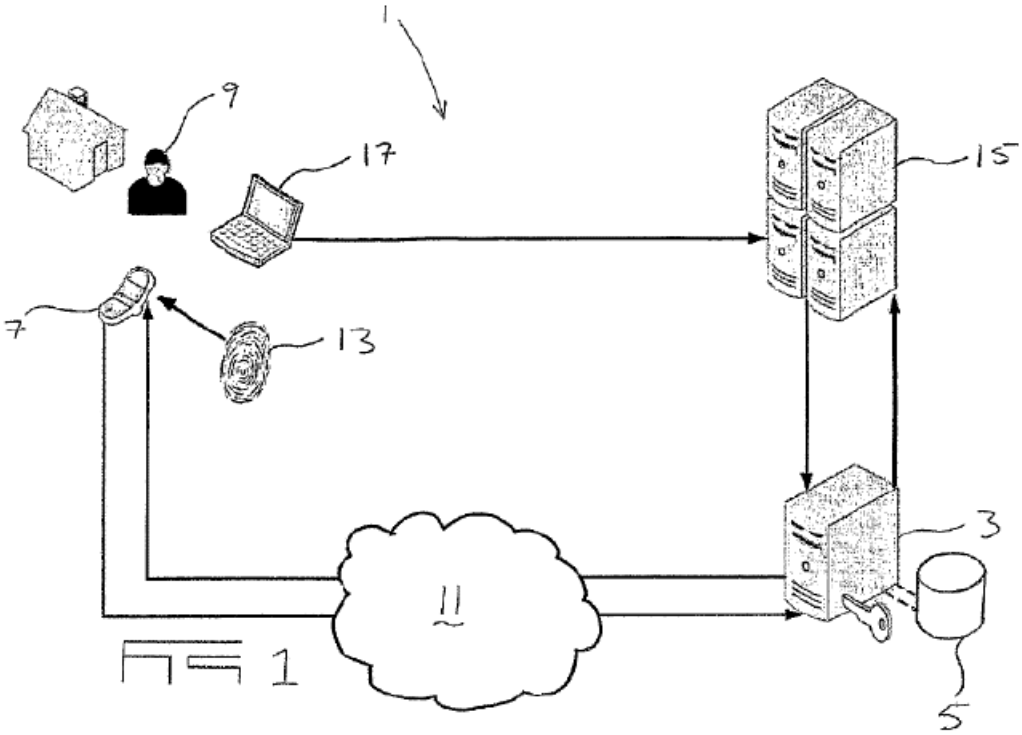
C. Description of Prior Art References

Petitioner's challenge primarily relies on Brand, Williams, Deibert, and Rahman. *See* Pet. 13. The remaining references (Partovi, Carter, and Russell) are relied on as additional secondary references to address certain specific limitations in the dependent claims.

1. Brand (Exhibit 1005)

Brand is a patent titled "Secure Transaction Authentication." Ex. 1005, code (54). Brand discloses a system "for authenticating secure

transactions between a transacting user and a secure transaction host." Ex. 1005, Abstract. Figure 1, reproduced below, shows Brand's authentication system including a user (9), user's computer (17), banking institution (15), user's mobile phone (7), and authentication server (3). Ex. 1005, 5:44, 6:48–55.



Ex-1005, FIG. 1

Figure 1 above, shows Brand's authentication system. Brand discloses that "to log into his or her internet banking account, the user (9) first accesses the website of the banking institution (15) at which his or her account is held, from a personal computer (17), laptop or other Internet enabled device." Ex. 1005, 6:47–50. The user "enters his account number (equivalent to a username) and password on the Internet banking website on his computer." Ex. 1005, 6:50–53.

"Before proceeding to login, the user (9) initiates the authentication application on his/her mobile phone." Ex. 1005, 6:53–55. The

authentication application establishes a "real-time communication link" via "a GSM network" between "the authentication server" and "the mobile phone." Ex. 1005, 6:62–64, 5:67.

"Upon the user (9) requesting login to his internet banking account, the banking institution (15) requests authentication of the user (9) from the authentication server." Ex. 1005, 7:1–3. The authentication server "sends a transaction confirmation request to the mobile phone (7) which is received by the software application." Ex. 1005, 7:3–6. The "software application triggers a pop-up on the monitor of the mobile phone" which allows "the user (9) to either confirm (accept) or deny (reject) the transaction." Ex. 1005, 7:6–12.

If the user "confirms the transaction, the application communicates this confirmation result to the server" which "sends a positive authentication result to the banking institution server." Ex. 1005, 7:12–15. The banking institution then allows the user "to proceed to its Internet banking account." Ex. 1006, 7:15–17.

2. Williams (Ex. 1006)

Williams is a patent titled "Electronic Payment Authorisation Using a Mobile Communications Device." Ex. 1006, (54). Williams relates to "a transaction authorisation system for electronic payments." Ex. 1006, 8.[1] Williams teaches that terminals are "linked to a card issuer's central transaction processing unit." *Id.* If the amount of a transaction is above some threshold, the authorization of the transaction is suspended until it can be authorized. *Id.* at 9. The transaction processing unit has an authorization

[1] This decision cites to the original page numbers not the page numbers added to the Exhibit.

module which causes a message generation module to transmit "a SMS message identifying the card account, the transaction data and time, the merchant and the transaction value..." to "a mobile communication device . . . for the card account." *Id.* The account holder "sends a return SMS message . . . using his mobile device." *Id.* at 10. If the "return SMS message is received within a predetermined period of time, the authorisation module 3 instructs the transaction processing unit 2 to authorise the transaction." *Id.* at 11.

3. Deibert (Ex. 1007)

Deibert is a patent titled "Mobile Phone Payment with Disabling Feature." Ex. 1007, code (54). Deibert relates to "contactless" mobile device payments. *Id*. at Abstract. Deibert describes mobile payment applications which allow wireless transmission of data allowing a payment transaction. *Id*. at 6:45–48. In Deibert, the user authenticates himself by providing a single authentication factor (i.e., "entering a password into the mobile phone application, in order to authenticate the consumer 30 and prevent fraud." (*id*. at 9:28–30)). If authentication is successful, the user's mobile phone executes a payment application "that stores payment details, such as a credit card number and related information." *Id*. at 2:49–51. For example, when a user wishes to make a purchase, he places his mobile phone "in proximity to an access device associated with the merchant. The mobile payment application may then send the payment details to the access device over a wireless connection." *Id*. at 2:51–55. Deibert also discloses that when the mobile phone is ready to conduct a transaction, the phone begins counting down from a predetermined timeout time. *Id*. at 9:30–38. If no payment transaction occurs before the timeout time elapses, the mobile payment application is disabled or deactivated. *Id*. at 9:38–40. Thus,

Deibert includes "a timer that automatically deactivates any mobile payment application[] after a predetermined timeout time has elapsed." *Id*. at 6:50–52.

4. Carter (Exhibit 1008)

Carter is a patent titled "Multifactor Authentication." Ex. 1008, code (54). Carter generally relates to authenticating transactions with a mobile device. *Id.* at Abstract. Carter also teaches "[a] standard cellular phone (referred to as MS) with a built-in or connected GPS or equivalent receiver (or other location determining capability)." *Id.* ¶ 104.

5. Rahman (Exhibit 1011)

Rahman is a patent titled "System and Method for Using Multiple Subscriber Identities to Provide Differentiated Services to Subscribers." Ex. 1011, code (54). Rahman generally relates to mobile stations with subscriber identities for establishing "wireless communication" with multiple networks. *Id.* at 3:6–14.

Rahman also teaches a mobile station that includes a "transceiver (XCVR)," a "microprocessor," and a "speaker." Ex. 1011, 17:5, 17:61–63, 16:61–63. The mobile station includes physical or user interface elements, e.g. keypad, stylus, touch sensitive display, for "user input selections." *Id.* at 17:49–59.

6. Partovi (Exhibit 1012)

Partovi is a patent titled "System and Methods for Inductive Charging, and Improvements and Uses Thereof." Ex. 1012, code (54). Partovi generally relates to charging techniques. Ex. 1012, Abstract. Partovi teaches that "mobile devices incorporate rechargeable batteries" and charging the mobile devices "through . . . USB or mini usb connector." Ex. 1012, ¶¶ 66, 69.

7. Russell (Exhibit 1013)

Russell is a patent titled "Biometric Identification Device." Ex. 1013, code (54). Russell relates to security that "limit[s] the transfer and distribution of personal data." *Id.* at Abstract. Russell teaches a portable device (PID) that includes a "self-destruct element 153 that destroys the identity data if unauthorized access to the stored identity data is attempted." *Id.* at 16:67–17:2.

III. ANALYSIS OF THE CHALLENGED CLAIMS

A. Obviousness

A claim is unpatentable under 35 U.S.C. § 103(a) if the differences between the claimed subject matter and the prior art are such that the subject matter, as a whole, would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations, including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in the art; and (4) where in evidence, so-called "secondary considerations," including commercial success, long-felt but unsolved needs, failure of others, and unexpected results. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966) ("the *Graham* factors").

B. Petitioner's Contentions Regarding Claim 1 based on Brand, Williams, and Deibert

Although claim 1 is not included in a ground in the Petition, Petitioner contends these the limitations of claim 1 would have been obvious over the combination of Brand, Williams, and Deibert, which is necessary to show that the challenged claims, which depend from claim 1, would have been

obvious over combinations including Brand, Williams, and Deibert. Pet. 15–24. Petitioner supports this assertion with testimony from its expert, Dr. McDaniel. McDaniel Decl. ¶¶ 75–93.

1. Rationale to Combine

a. Brand and Deibert

Petitioner also argues that a person of ordinary skill would have been motivated to combine Brand and Deibert. Pet. 20–23. Petitioner contends that both Brand and Deibert describe authentication features that prevent fraud. Pet. 20–21 (citing McDaniel Decl. ¶ 84; Ex. 1005, Abstract; Ex. 1007, 9:27–30). Petitioner asserts that after Brand initiates an authentication application, a person of ordinary skill in the art at the time of the invention would have known that the application continues until the phone loses power or the application is deactivated. Id. (citing McDaniel Decl. ¶ 84; Ex. 1005, 6:53–54). Thus, according to Petitioner a person of ordinary skill in the art at the time of the invention would recognize automatically deactivating an authentication application would be desirable. *Id.* (citing McDaniel Decl. ¶ 85). In other words, Petitioner suggests deactivating the application would save battery life.

According to Petitioner, Deibert teaches software "code relating to a timer that automatically deactivates any mobile payment applications after a predetermined timeout time has elapsed." Pet. 21 (quoting Ex. 1007, 6:49–53). Petitioner contends that adding Deibert's automatic deactivation feature to Brand would make Brand's application easier to use than with manual deactivation, and would also increase security because the user would otherwise have to reinitialize the application with the user's credentials if it deactivates. *Id.* at 21–22 (citing McDaniel Decl. ¶¶ 86–89). Petitioner also asserts a person of ordinary skill in the art at the time of the invention would

recognize the predetermined time would start either when the authentication application is initiated or when the requested transaction is confirmed or denied. *Id.* at 22–23 (citing McDaniel Decl. ¶ 90).

Petitioner further contends a person of ordinary skill in the art at the time of the invention would have had a reasonable expectation of success in making the combination. *Id.* at 23. Petitioner asserts a [person of ordinary skill in the art at the time of the invention] would have been familiar with conventional coding languages in order to code the combination and thus the "combination is simply combining prior art elements (Deibert's timer that automatically deactivates Brand's authentication application) according to known methods (code written in a programming language) to yield predictable results (automatically deactivating the authentication application)." *Id.* (citing McDaniel Decl. ¶ 91). Petitioner supports these assertions with testimony from Dr. McDaniel. *See* McDaniel Decl. ¶¶ 83–91.

Patent Owner responds that a person of ordinary skill in the art at the time of the invention would not have added Deibert's automatic deactivation to Brand. Prelim. Resp. 39. Specifically, Patent Owner argues that deactivation and the necessary associated reinitialization would frustrate Brand's purpose of allowing multiple transactions in one session and Deibert's purpose to allowing the user to interact with the system by logging on only once. *Id.* at 41–42 (citing Ex. 1005, 7:18–24; Ex. 1007, 9:45–53). Patent Owner further argues that adding such a feature could deactivate the pop-up notification of Brand and prevent the user from manually confirming or denying a transaction. *Id.* at 39.

Patent Owner relies on Brand's statement that a session can last though subsequent transactions (i.e., continuous and ongoing) depending on

"the type of transaction that the user (9) attempts to perform and the decision of the bank on how to implement the security layer provided by the invention." *Id.* at 41–42 (citing Ex. 1005, 7:21–24). Therefore, Patent Owner suggests, the intent in Brand is to allow an open session with multiple transactions. *Id.*

Patent Owner further argues that Brand and Deibert are directed to "completely different aspects of a payment system" because, among other things, Brand is directed to a two-factor authentication system whereas Deibert is directed to a one factor authentication system. Prelim. Resp. 40. Additionally, Patent Owner argues that Petitioner's asserted motivations of increasing security and making the system easier to use are inconsistent with each other because additional security inevitably involves making the system harder to use. *Id.* at 41.

Patent Owner also asserts that Deibert's teaching that there is a "code relating to a timer that automatically deactivates *any mobile payment application*" is directed to payment applications not authentication applications. Prelim. Resp. 42–43. In Deibert, deactivation is directed to the mobile payment applications--the payment application facilitates payment transaction and must be running for the transaction to be completed. *Id.* In fact, the" "mobile payment application in Deibert serves a different function than the "authentication application" in Brand--i.e. Deibert's mobile payment application simply completes a transaction, but Brand's authentication application performs the act of confirming or denying the transaction. In Brand, authentication application must be running for the user to receive the pop-up which confirms the transaction (Pet. 35 (citing Ex. 1005, 7:6–15, 7:25–29), while in Deibert the transaction is already authorized and the mobile payment application must be running only to send

the contactless transaction to the terminal (*see* Ex. 1007, 3:57–59); *see also* Pet. 21 (discussing Deibert's deactivation function).

We agree with Patent Owner that Brand and Deibert operate in different ways (i.e. one-factor vs. two-faction authentication) and Petitioner combines different functions (mobile payment vs authentication) without explaining sufficiently why those functions would be combined. We are also not persuaded by Petitioner's conclusory references to saving battery life, making Brand's application easier to use, and increasing security—particularly when balanced against the fact that Deibert's deactivation conflicts with Brand's stated ability to hold a session open through multiple transactions.

Finally, Patent Owner argues that the combination would not be "combining prior art elements . . . according to known methods . . . to yield predictable results." Prelim. Resp. 43–44. We agree. We are also not persuaded by Petitioner's assertion that because both Brand and Deibert are implemented in programming code, it would be a simple combination. Pet. 23. This statement, by itself, does not provide any rationale for combining the cited teachings and certainly does not provide a sufficiently "articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." *KSR*, 550 U.S. at 418 (quoting *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)).

In summary, based on the information set forth in the Petition and the testimony of Dr. McDaniel, we are not persuaded that Petitioner has demonstrated sufficiently both the motivation to combine these references and the reasonable expectation of success as to its ground based on Brand, Williams, and Deibert.

b. Brand and Williams

Petitioner argues that a person of ordinary skill would have been motivated to combine Brand and Williams. Pet. 18–21. Petitioner contends Brand and Williams are both directed to payment transaction authorization and two-factor authentication. Pet. 18 (citing Ex. 1005, Abstract, 10:59–62; Ex. 1006, Abstract, 8–11; McDaniel Decl. ¶ 76).

Petitioner argues Brand's two factor authentication using a mobile phone is "desirable." *Id.* Specifically, according to Petitioner, [a person of ordinary skill in the art "would have recognized such techniques are desirable, as they increase the authentication system's security and reduce fraud where a third-party, acting as a user, initiates a transaction." *Id.* (citing McDaniel Decl. ¶ 77).

Petitioner contends that Williams' system of sending an SMS message to confirm transactions improves security. Pet. 19. Petitioner states "Williams' predetermined period of time during which a transaction may be authorized improves the security of Williams' system and assists in preventing the authorization of fraudulent transactions. Without any such time limit, a requested transaction would remain pending until the user responds. This could lead to the user unintentionally or mistakenly approving a transaction that the user did not request (i.e., a fraudulent transaction)." *Id.* (internal citations omitted (citing McDaniels Decl. ¶ 70)).

As to the motivation to combine Brand and Williams, Petitioner argues it would have been obvious to a person of ordinary skill in the art to employ a time limit (i.e., similar to Williams's time limit) in Brand's system, such that a user would have a limited period of time to validate that the user possesses the mobile device. Pet. 19 (citing Ex. 1003 ¶ 79). According to Petitioner:

> This would contribute to the overall security of the authentication system. Including a predetermined time period is a way to validate that the user possessed the mobile device between the time the user initiated the transaction at his computer and the transaction was confirmed (or denied) at the authentication server. Ex-1003, ¶ 80; Ex-1005, 10:48-50. If the authentication server has not received a confirmation message after the predetermined time interval expired, the authentication server would determine that the transaction is fraudulent. Ex-1003, ¶ 80. When a user does not approve a transaction in a timely manner, there is an increased risk that the transaction is fraudulent. Ex-1003, ¶ 80.

Id. at 19–20 (citing McDaniel Decl. ¶ 80). Additionally, according to Petitioner, it was known in the art that security is enhanced "by limiting the time when authentication is possible." *Id.* at 20 (quoting Ex. 1014, 17:4–5 (a supporting prior art reference (McCorkle) that is not part of the ground).

Finally, Petitioner contends a person of ordinary skill in the art would have had a reasonable expectation of success in making the combination. *Id.* at 20. Petitioner asserts "such a combination would have simply been combining prior art elements (Williams' time-limited window for responding and Brand's accept/deny message) according to known methods (rejecting transactions for which a timely response is not received) to yield predictable results (validating that the user possesses the mobile device at the time of a transaction)." *Id.* at 20 (citing McDaniel Decl. ¶ 81). Petitioner further argues the combination of Brand and Williams is "merely the ordinary use of a common technique (limiting the time window for approving a transaction) to improve a similar two-factor authentication system in the same way (reducing fraudulent transactions)." *Id.* Petitioner supports these assertions with testimony from Dr. McDaniel. *See* McDaniel Decl. ¶¶ 75–81.

Patent Owner responds that Petitioner's argument for combining the references, as supported by Dr. McDaniel, are based on hindsight. Prelim. Resp. 53. Petitioner also asserts that "[w]hile Brand and Williams are generally related to payment transaction authorization, Brand explicitly discourages the use of Williams's SMS messaging application and teaches away from such an implementation." Prelim. Resp. 51. Patent Owner cites Brand as "disparag[ing]" SMS messaging applications calling them "susceptible to abuse," "relatively high cost" and "prone to 'mistakes.'" *Id.* Patent Owner also asserts that the one embodiment in Brand that uses an SMS message is not related to timing and is not cited by Petitioner. *Id.* Thus, according to Patent Owner, a person of ordinary skill "would not have combined Williams's SMS messaging system with Brand's system that forms its own direct, secure, and continuous connection between the mobile phone and the authentication server." *Id.* at 52.

Patent Owner asserts "a [person of ordinary skill in the art at the time of the invention], upon reading Brand and Williams, would . . . not have arrived at the claimed predetermined time relation." Prelim. Resp. 52. Patent Owner asserts that a person of ordinary skill in the art at the time of the invention would be led to an alternate solution, i.e., "would have implemented a system that counts down the time for Brand's user to select accept or deny on the pop-up notification on the user's mobile phone. That timer would have begun at the time that the pop-up notification appears on the user's mobile phone, not at a time that the user identification is transmitted over the first communication channel or a response is transmitted over a second communication channel." Prelim. Resp. 52–53.

We also agree with Patent Owner that the timer in Williams is used for a purpose, i.e., SMS messaging, that Brand disparages. Prelim. Resp.

51–52. We also agree with Patent Owner that Petitioner's arguments regarding motivation to combine the references are based on hindsight. Prelim. Resp. 53. For example, as explained further in Section III.B.2., *infra*, Petitioner does not explain why the predetermined time would start when the user enters their identification in a system when combining a direct message system with a system based on SMS messages and when neither reference has any disclosure about the start of the predetermined time. Thus, we are not persuaded that Petitioner's articulated reasoning for why one of ordinary skill in the art would have been motivated to make the proposed combination is based on rational underpinnings. *See KSR Int'l Co.*, 550 U.S. at 418.

Petitioner's expert's declarant (McDaniel Decl. ¶¶ 75–81) essentially repeats the assertions of the Petition and provides no persuasive facts or data to support his opinion of obviousness. Therefore, we give such conclusory, unsupported assertions by Petitioner's expert little weight. *See In re Am. Acad. of Sci. Tech Ctr.*, 367 F.3d 1359, 1368 (Fed. Cir. 2004) ("[T]he Board is entitled to weigh the declarations and conclude that the lack of factual corroboration warrants discounting the opinions expressed in the declarations."); *see also* 37 C.F.R. § 42.65(a) ("Expert testimony that does not disclose the underlying facts or data on which the opinion is based is entitled to little or no weight.").

We are also not persuaded by Petitioner's assertion that the combination of Brand and Williams would have simply been combining prior art elements according to known methods to yield predictable results. This statement, by itself, does not provide any rationale for combining the cited teachings and certainly does not provide a sufficiently "articulated reasoning with some rational underpinning to support the legal conclusion of

obviousness." *KSR*, 550 U.S. at 418 (quoting *Kahn*, 441 F.3d at 988). Petitioner does not explain persuasively how or why a person of ordinary skill would have combined the cited teachings. *See KSR*, 550 U.S. at 418 ("Often, it will be necessary for a court to . . . determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue.").

In sum, we are not convinced that Petitioner has presented a sufficient rationale, apart from hindsight, demonstrating that a person of ordinary skill would have combined Brand with Deibert and/or Williams.

2. Teaching of Claim Limitations

In addition, even if Petitioner had sufficiently demonstrated that Brand, Williams, and Deibert would have been combined, the references in combination still would fail to teach or suggest at least one element of the challenged claims. Specifically, independent claim 1 recites, in relevant part, "as a criterion for deciding whether the authentication to the transaction shall be granted or denied, having the authentication device check whether a predetermined time relation exists between the transmission of the user identification and a response from the second communication channel," ("time window limitation"). Pet. 29–33. Petitioner has failed to persuade us that the references relied on in the Petition disclose this claimed feature.

Petitioner relies on the combination of Brand and Williams to meet this limitation. *Id.* Petitioner relies on Brand's teaching that authentication where a pop-up of the authentication application "requests the user (9) to either confirm (accept) or deny (reject) the transaction by means of an appropriate key press," and communicates a "result to [authentication] server" as the claimed deciding whether the authentication to the transaction shall be granted or denied. *Id.* at 29 (citing Ex. 1005, 7:6–13, 7:25–27).

Petitioner also relies on Williams' authorization module which checks if a "**return SMS message is received within a predetermined period of time**," as the claimed criterion. *Id.* (citing Ex. 1006, 11). As to the limitation "[a predetermined time relation exists] between the transmission of the user identification and a response," Petitioner relies on Williams's teaching that "a user 'entering data concerning a transaction,' e.g. a card name and number [*see* Ex. 1006, 9–10], and then transmitting a 'notification message to a predetermined mobile communication device.'" Pet. 31–33 (citing Ex. 1006, 6). Additionally, Petitioner states:

> It would have been obvious to a [person of ordinary skill in the art at the time of the invention] that this "predetermined period of time" would be measured from when the transaction was first initiated, i.e., starting at *the transmission of the user identification*. Ex-1003, p. 54.

Id. at 31. In other words, Petitioner relies on the knowledge of one of ordinary skill to show that the start of the predetermined time in Williams would be when the user information was sent. *Id.*[2]

Patent Owner asserts Williams's timer would not meet the limitation to starting the timer's predetermined time relation at "transmission of the user identification" because "William's [sic] timer begins counting down when the initial notification SMS message is sent to the phone, not when the user provides his user identification." Prelim. Resp. 48. Patent Owner acknowledges that Petitioner relies on the knowledge of one of ordinary skill in the art on page 32 of the Petition, but argues that "Petitioner and its expert have failed to show that the [person of ordinary skill in the art at the time of the invention] ***would have, not just could have,*** made the modification of

[2] The alleged motivation to combine these teachings is discussed in Section III.B.1.b., *supra*.

the prior art to arrive at the claimed invention. Prelim. Resp. 49 (citing *Belden Inc. v. Berk-Tek LLC*, 805 F.3d 1064, 1073 (Fed. Cir. 2015)[3]; *Metalcraft of Mayville, Inc. v. Toro Co.*, 848 F.3d 1358, 1367 (Fed. Cir. 2017)[4].

Ultimately, Petitioner asserts:

> It would have been obvious to a [person of ordinary skill in the art at the time of the invention] to determine whether the time that Brand's user transmitted user information to the banking institution and the time the user transmitted a confirmation or denial result to the authentication server falls within the predetermined time period taught in Williams. Ex-1003, p. 55. This would make the authentication system more secure by adding a safeguard that validates that a person possessed the mobile device when the transaction was initiated and authenticated. It would also reduce fraudulent transactions because transactions would not authenticate if the time interval exceeds the predetermined time period. Ex-1003, p. 55. *See* Reasons to Combine Brand and Williams, § IX.C.4.

Id. at 32. In other words, Petitioner appears to state that, although neither Brand nor Williams teaches the time window limitation of the claims, one of ordinary skill would have been motivated to modify Brand to add the claimed time window to make the transaction more secure. We determine that this contention by Petitioner is speculative and based on hindsight. Petitioner's does not meet the standard set forth by the authorities requiring "specific reasoning, based on evidence of record, to support the legal conclusion of obviousness." *In re Magnum Oil Tools Int'l, Ltd.*, 829 F.3d

[3] Patent Owner cited "*Belden Inc. v. Berk-Tek LLC*, No. 14-1575 (Fed. Cir. 2015) 2015." Prelim. Resp. 49.
[4] Patent Owner cites this case as "*Metalcraft of Mayville, Inc. v. The Toro Company*, No.-16-2433 (Fed. Cir. 2017)." Prelim. Resp. 49.

1364, 1380 (Fed. Cir. 2016). Thus, we are not persuaded by Petitioner's arguments.

Petitioner's expert essentially repeats the assertions of the Petition and provides no persuasive facts or data to support his opinion that the combination of Brand and Williams teaches these claim limitations. We give such conclusory, unsupported assertions by Petitioner's expert little weight. *See In re Am. Acad. of Sci. Tech Ctr.*, 367 F.3d at 1368 ("[T]he Board is entitled to weigh the declarations and conclude that the lack of factual corroboration warrants discounting the opinions expressed in the declarations."); *see also* 37 C.F.R. § 42.65(a) ("Expert testimony that does not disclose the underlying facts or data on which the opinion is based is entitled to little or no weight."); *Seabery N. Am., Inc. v. Lincoln Glob., Inc.*, IPR2016–00749, Paper 13 at 14 (PTAB Sept. 21, 2016) (Institution Decision). In the absence of persuasive argument or evidence, we determine Petitioner has failed to adequately show the combination of Brand and Williams teaches or suggests this limitation to a person of ordinary skill.

For at least the reasons discussed above, Petitioner has not demonstrated a reasonable likelihood of prevailing on its obviousness challenge based on Brand, Williams, and Deibert.

C. Challenge to Claims 14, 21, 24, 25, and 26 based on Brand, Williams, Deibert, and Rahman

Petitioner contends these claims would have been obvious over the combination of Brand, Williams, Deibert, and Rahman. Pet. 38–68. Petitioner supports this assertion with testimony from Dr. McDaniel. McDaniel Decl. ¶¶ 143–191.

Patent Owner argues that Rahman does not remedy the deficiencies of Brand, Williams, and Deibert as to teaching the limitations of claim 1.

Prelim. Resp. 54. We agree. Petitioner does not rely on Rahman as curing any of the deficiencies discussed above. Thus, based on the information set forth in the Petition and the testimony of Dr. McDaniel, we are not persuaded that Petitioner has demonstrated sufficiently both the motivation to combine these references and the reasonable expectation of success as to its ground based on Brand, Williams, Deibert, and Rahman.

D. Challenge to Claims 15–17 based on Brand, Williams, Deibert, Rahman, and Partovi

Petitioner contends these claims would have been obvious over the combination of Brand, Williams, Deibert, Rahman, and Partovi. Pet. 68–75. Petitioner supports this assertion with testimony from its expert, Dr. McDaniel. McDaniel Decl. ¶¶ 192–211.

Patent Owner argues that Partovi does not remedy the deficiencies of Brand, Williams, Deibert, and Rahman as to teaching the limitations of claim 1. Prelim. Resp. 54–55. We agree. Petitioner does not rely on Partovi as curing any of the deficiencies discussed above. Thus, based on the information set forth in the Petition and the testimony of Dr. McDaniel, we are not persuaded that Petitioner has demonstrated sufficiently both the motivation to combine these references and the reasonable expectation of success as to its ground based on Brand, Williams, Deibert, Rahman, and Partovi.

E. Challenge to Claim 19 based on Brand, Williams, Deibert, Rahman, and Carter

Petitioner contends these claims would have been obvious over the combination of Brand, Williams, Deibert, Rahman, and Carter. Pet. 76–80. Petitioner supports this assertion with testimony from its expert, Dr. McDaniel. McDaniel Decl. ¶¶ 212–213.

Patent Owner argues that Carter does not remedy the deficiencies of Brand, Williams, Deibert, and Rahman as to teaching the limitations of claim 1. Prelim. Resp. 55. We agree. Petitioner does not rely on Carter as curing any of the deficiencies discussed above. Thus, based on the information set forth in the Petition and the testimony of Dr. McDaniel, we are not persuaded that Petitioner has demonstrated sufficiently both the motivation to combine these references and the reasonable expectation of success as to its ground based on Brand, Williams, Deibert, Rahman, and Carter.

E. Challenge to Claim 22 based on Brand, Williams, Deibert, Rahman, and Russell

Petitioner contends these claims would have been obvious over the combination of Brand, Williams, Deibert, Rahman, and Russell. Pet. 80–83. Petitioner supports this assertion with testimony from its expert, Dr. McDaniel. McDaniel Decl., 214–223.

Patent Owner argues that Russell does not remedy the deficiencies of Brand, Williams, Rahman, and Deibert as to teaching the limitations of claim 1. Prelim. Resp. 56–57. We agree. Petitioner does not rely on Russell as curing any of the deficiencies discussed above. Thus, based on the information set forth in the Petition and the testimony of Dr. McDaniel, we are not persuaded that Petitioner has demonstrated sufficiently both the motivation to combine these references and the reasonable expectation of success as to its ground based on Brand, Williams, Deibert, Rahman, and Russell.

IV. CONCLUSION

We determine that Petitioner has not demonstrated a reasonable likelihood of prevailing on its challenges to claims 14–17, 19, 21, 22, and 24–26 of the '903 patent.

V. ORDER

Upon consideration of the record before us, it is:

ORDERED that the Petition is DENIED and no trial is instituted.

IPR2019-01639
Patent 9,246,903 B2

FOR PETITIONER:

David McCombs
Theodore Foster
Dina Blikshteyn
HAYNES AND BOONE, LLP
david.mccombs.ipr@haynesboone.com
ipr.theo.foster@haynesboone.com
dina.blikshteyn.ipr@haynesboone.com

FOR PATENT OWNER:

Scott Weingaertner
Grace Wang
WHITE & CASE LLP
scott.weingaertner@whitecase.com
grace.wang@whitecase.com